L Number	Hits	Search Text	DB	Time stamp
1	112486	encryption or encipher or encode	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:26
8	66895	stor$3 adj3 address	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:27
15	91510	stor$3 near3 address	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:27
22	54088	stor$3 near3 $3location	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:28
29	118967	decryption or decipher or decode	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:29
36	128561	(stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:29
43	5418	((stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)) same ((encryption or encipher or encode) or (decryption or decipher or decode))	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:55
50	29746	(713/$ or 705/$ or 380/$).ccls	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:34
57	569	(((stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)) same ((encryption or encipher or encode) or (decryption or decipher or decode))) and ((713/$ or 705/$ or 380/$).ccls)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:35
64	496	(((stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)) same ((encryption or encipher or encode) or (decryption or decipher or decode))) and ((713/$ or 705/$ or 380/$).ccls) and (decryption or decipher or decode)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:47
71	19905	(magnetic or optical) adj (media or medium)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:49
78	22	((((stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)) same ((encryption or encipher or encode) or (decryption or decipher or decode))) and ((713/$ or 705/$ or 380/$).ccls) and (decryption or decipher or decode)) and ((magnetic or optical) adj (media or medium))	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:49
85	150837	(magnetic or optical) adj (media or medium) or cd or cdrom or cd-rom	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:50

92	150837	((magnetic or optical) adj (media or medium)) or cd or cdrom or cd-rom	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:51
99	22	(((((stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)) same ((encryption or encipher or encode) or (decryption or decipher or decode))) and ((713/$ or 705/$ or 380/$).ccls) and (decryption or decipher or decode)) and ((magnetic or optical) adj (media or medium))) and (((magnetic or optical) adj (media or medium)) or cd or cdrom or cd-rom)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:51
106	1	(((((stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)) same ((encryption or encipher or encode) , or (decryption or decipher or decode))) and ((713/$ or 705/$ or 380/$).ccls) and (decryption or decipher or decode)) and "9278" and (((magnetic or optical) adj (media or medium)) or cd or cdrom or cd-rom)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:51
113	100	(((((stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)) same ((encryption or encipher or encode) or (decryption or decipher or decode))) and ((713/$ or 705/$ or 380/$).ccls) and (decryption or decipher or decode)) and (((magnetic or optical) adj (media or medium)) or cd or cdrom or cd-rom)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:52
120	135975	memory near3 $3location or memory near3 address	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:54
127	204808	((stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)) or (memory near3 $3location or memory near3 address)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:54
134	11462	(((stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)) or (memory near3 $3location or memory near3 address)) same ((encryption or encipher or encode) or (decryption or decipher or decode))	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:55
141	1020	((((stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)) or (memory near3 $3location or memory near3 address)) same ((encryption or encipher or encode) or (decryption or decipher or decode))) and ((713/$ or 705/$ or 380/$).ccls)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 10:56
148	188	(((((stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)) or (memory near3 $3location or memory near3 address)) same ((encryption or encipher or encode) or (decryption or decipher or decode))) and ((713/$ or 705/$ or 380/$).ccls)) and (((magnetic or optical) adj (media or medium)) or cd or cdrom or cd-rom)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 11:04
155	58126	access$3 near3 (prohibit or prevent$3 or permit or permission)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB	2001/08/10 11:06

| 162 | 54 | ((((((stor$3 adj3 address) or (stor$3 near3 address) or (stor$3 near3 $3location)) or (memory near3 $3location or memory near3 address)) same ((encryption or encipher or encode) or (decryption or decipher or decode))) and ((713/$ or 705/$ or 380/$).ccls)) and (((magnetic or optical) adj (media or medium)) or cd or cdrom or cd-rom)) and (access$3 near3 (prohibit or prevent$3 or permit or permission)) | USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM TDB | 2001/08/10 11:06 |

	U	1	Document ID	Issue Date	Pages
1	☐	☐	US 20010001014 A1		51
2	☐	☐	US 6260120 B1	20010710	66
3	☐	☐	US 6253193 B1	20010626	319
4	☒	☐	US 6252964 B1	20010626	47
5	☒	☐	US 6250548 B1	20010626	54
6	☒	☐	US 6246767 B1	20010612	49
7	☒	☐	US 6237786 B1	20010529	316
8	☒	☐	US 6202054 B1	20010313	84
9	☒	☐	US 6192130 B1	20010220	15

	Title	Current OR	Current XRef
1	Source authentication of download information in a conditional access system		
2	Storage mapping and partitioning among multiple host processors in the presence of login state changes and host controller replacement	711/152	707/101 ; 707/3 ; 707/4 ; 707/5 ; 711/147 ; 711/149 ; 711/153 ; 711/170
3	Systems and methods for the secure transaction management and electronic rights protection	705/57	705/52
4	Authorization of services in a conditional access system	380/282	380/2 ; 380/223
5	Electronic voting system	235/51	
6	Source authentication of download information in a conditional access system		380/232 ; 380/282 ; 380/285 ; 380/30 ; 380/43 ; 713/153 ; 713/168
7	Systems and methods for secure transaction management and electronic rights protection	213/153	380/203 ; 705/51 ; 705/58
8	Method and system for remote delivery of retail banking services	705/42	705/26 ; 705/35 ; 705/39
9	Information security subscriber trust authority transfer system with private key history transfer	380/277	380/1 ; 380/280 ; 380/286 ; 705/66 ; 705/71 ; 705/76 ; 713/157 ; 713/158 ; 713/178

	Retrieval Classif	Inventor	S	C	P
1		Akins, Glendon L. III , Banker, Robert O. , et al.	☒	☐	☐
2		Blumenau, Steven M. , et al.	☒	☐	☐
3		Ginter, Karl L. , et al.	☒	☐	☐
4		Wasilewski, Anthony J. , et al.	☐	☐	☐
5		McClure, Neil , et al.	☐	☐	☐
6		Akins, III, Glendon L. , et al.	☐	☐	☐
7		Ginter, Karl L. , et al.	☐	☐	☐
8		Lawlor, Matthew P. , et al.	☐	☐	☐
9		Otway, Josanne	☐	☐	☐

	U	1	Document ID	Issue Date	Pages
10	☒	☐	US 6185686 B1	20010206	21
11	☒	☐	US 6157719 A	20001205	51
12	☒	☐	US 6122716 A	20000919	32
13	☒	☐	US 6118870 A	20000912	11
14	☒	☐	US 6115823 A	20000905	66
15	☒	☐	US 6105134 A	20000815	49
16	☒	☐	US 6091884 A	20000718	243
17	☒	☐	US 6052468 A	20000418	16
18	☒	☐	US 6052780 A	20000418	23

		Title	Current OR	Current XRef
10		Computer system and process for accessing an encrypted and self-decrypting digital information product while restricting access to decrypted digital	713/190	380/255 ; 380/264 ; 713/193
11		Conditional access system	380/210	725/31
12		System and method for authenticating a computer memory	711/163	365/185.04 ; 711/154 ; 713/190
13		Microprocessor having instruction set extensions for decryption and multimedia applications	380/201	345/202 ; 380/200 ; 382/166 ; 382/232 ; 713/182 ; 713/189 ; 713/193 ; 713/200 ; 713/201
14		System and method for task performance based dynamic distributed power management in a computer system and design method therefor	713/322	710/16 ; 710/18 ; 710/9 ; 713/300 ; 713/310 ; 713/323 ; 713/324
15		Verification of the source of program information in a conditional access system	713/170	380/239 ; 380/241 ; 380/279 ; 713/168
16		Enhancing operations of video tape cassette players	386/83	386/46 ; 386/95
17		Method of securing a cryptographic key	380/281	713/194
18		Computer system and process for accessing an encrypted and self-decrypting digital information product while restricting access to decrypted digital	713/193	380/255 ; 380/287 ; 713/150 ; 713/182 ; 713/189 ; 713/190 ; 713/200

	Retrieval Classif	Inventor	S	C	P
10		Glover, John J.	☐	☐	☐
11		Wasilewski, Anthony J. , et al.	☐	☐	☐
12		Combs, James Lee	☐	☐	☐
13		Boyle, Douglas B. , et al.	☐	☐	☐
14		Velasco, Francisco , et al.	☐	☐	☐
15		Pinder, Howard G. , et al.	☐	☐	☐
16		Yuen, Henry C. , et al.	☐	☐	☐
17		Hillhouse, Robert D.	☐	☐	☐
18		Glover, John J.	☐	☐	☐

	U	1	Document ID	Issue Date	Pages
19	☒	☐	US 6047376 A	20000404	12
20	☒	☐	US 6044157 A	20000328	47
21	☒	☐	US 5987614 A	19991116	34
22	☒	☐	US 5982891 A	19991109	315
23	☒	☐	US 5958051 A	19990928	18
24	☒	☐	US 5949876 A	19990907	318
25	☒	☐	US 5950172 A	19990907	25
26	☒	☐	US 5917912 A	19990629	319
27	☒	☐	US 5915019 A	19990622	

	Title	Current OR	Current XRef
19	Client-server system, server access authentication method, memory medium stores server-access authentication programs, and issuance device which issues the memory medium	713/201	709/227 ; 713/202
20	Microprocessor suitable for reproducing AV data while protecting the AV data from illegal copy and image information processing system using	380/201	380/217 ; 713/189 ; 713/190
21	Distributed power management system and method for computer	713/300	710/16 ; 710/18 ; 710/9 ; 713/310 ; 713/323 ; 713/324
22	Systems and methods for secure transaction management and electronic rights protection	705/54	705/26 ; 713/167
23	Implementing digital signatures for data streams and data archives	713/200	
24	Systems and methods for secure transaction management and electronic rights protection	705/80	705/1 ; 705/39 ; 705/54
25	Secured electronic rating system	705/26	
26	System and methods for secure transaction management and electronic rights protection	713/187	705/40 ; 709/312 ; 713/164
27	Systems and methods for secure transaction management and electronic rights protection	705/54	705/26 ; 705/400 ; 713/200

	Retrieval Classif	Inventor	S	C	P
19		Hosoe, Makoto	☐	☐	☐
20		Uesaka, Yasushi , et al.	☐	☐	☐
21		Mitchell, Phillip Merle , et al.	☐	☐	☐
22		Ginter, Karl L. , et al.	☐	☐	☐
23		Renaud, Benjamin J. , et al.	☐	☐	☐
24		Ginter, Karl L. , et al.	☐	☐	☐
25		Klingman, Edwin E.	☐	☐	☐
26		Ginter, Karl L. , et al.	☐	☐	☐
27		Ginter, Karl L. , et al.	☐	☐	☐

	U	1	Document ID	Issue Date	Pages
28	☒	☐	US 5910987 A	19990608	
29	☒	☐	US 5907617 A	19990525	
30	☒	☐	US 5901327 A	19990504	
31	☒	☐	US 5892900 A	19990406	
32	☒	☐	US 5883955 A	19990316	
33	☒	☐	US 5870724 A	19990209	
34	☒	☐	US 5809145 A	19980915	
35	☒	☐	US 5765197 A	19980609	
36	☒	☐	US 5765176 A	19980609	

	Title	Current OR	Current XRef
28	Systems and methods for secure transaction management and electronic rights protection	705/52	705/30
29	Try before you buy software distribution and marketing system	705/52	705/27 ; 705/77 ; 713/200
30	Bundling of write data from channel commands in a command chain for transmission over a data link between data storage systems for remote	710/5	709/232 ; 711/100 ; 711/112
31	Systems and methods for secure transaction management and electronic rights protection	713/200	713/201
32	On-line try before you buy software distribution system	705/52	705/26 ; 705/57 ; 713/200
33	Targeting advertising in a home retail banking delivery service	705/42	235/379 ; 235/380 ; 705/14 ; 705/43
34	System for distributing digital information	705/52	705/77 ; 713/164 ; 713/201
35	Method and system for authentication of a memory unit for a computer system	711/164	380/42 ; 711/100 ; 711/163 ; 713/190 ; 713/200
36	Performing document image management tasks using an iconic image having embedded encoded information	707/514	345/634 ; 345/838 ; 707/529 ; 707/530

	Retrieval Classif	Inventor	S	C	P
28		Ginter, Karl L. , et al.	☐	☐	☐
29		Ronning, Joel A.	☐	☐	☐
30		Ofek, Yuval	☐	☐	☐
31		Ginter, Karl L. , et al.	☐	☐	☐
32		Ronning, Joel A.	☐	☐	☐
33		Lawlor, Matthew P. , et al.	☐	☐	☐
34		Slik, David , et al.	☐	☐	☐
35		Combs, James Lee	☐	☐	☐
36		Bloomberg, Dan S.	☐	☐	☐

	U	1	Document ID	Issue Date	Pages
37	☒	☐	US 5761698 A	19980602	
38	☒	☐	US 5724599 A	19980303	
39	☒	☐	US 5694469 A	19971202	
40	☒	☐	US 5677953 A	19971014	
41	☒	☐	US 5666516 A	19970909	
42	☒	☐	US 5533125 A	19960702	
43	☒	☐	US 5416840 A	19950516	
44	☒	☐	US 5394469 A	19950228	
45	☒	☐	US 5375243 A	19941220	
46	☒	☐	US 5220501 A	19930615	

	Title	Current OR	Current XRef
37	Computer system having audio/video/CD drive controller/coprocessor having integral memory interface, graphics coprocessor, digital signal processor, compact disk controller, and video	711/100	345/503 ; 345/520 ; 711/151 ; 711/154 ; 711/158 ; 711/3
38	Message passing and blast interrupt from processor	712/43	710/260 ; 710/264 ; 713/1 ; 714/23
39	Method and system for disseminating stored programs and data	705/51	340/5.74 ; 705/56 ; 713/193 ; 713/200
40	System and method for access control for portable data storage media	705/51	380/201 ; 380/231 ; 380/240 ; 713/193
41	Protected programmable memory cartridge having selective access circuitry	711/163	365/195 ; 711/152 ; 713/190 ; 713/200
42	Removable computer security device	711/163	713/193
43	Software catalog encoding method and system	705/52	380/277 ; 705/56
44	Method and apparatus for retrieving secure information from mass storage media	705/53	380/279 ; 380/29 ; 380/44
45	Hard disk password security system	713/202	380/52 ; 711/112 ; 711/164 ; 713/183 ; 713/193
46	Method and system for remote delivery of retail banking services	705/40	379/93.18 ; 380/29 ; 705/42 ; 705/43 ; 705/70 ; 705/77 ; 902/24

	Retrieval Classif	Inventor	S	C	P
37		Combs, James Lee	☐	☐	☐
38		Balmer, Keith , et al.	☐	☐	☐
39		Le Rue, Charles	☐	☐	☐
40		Dolphin, Janet L.	☐	☐	☐
41		Combs, James Lee	☐	☐	☐
42		Bensimon, Daniel , et al.	☐	☐	☐
43		Cane, David A. , et al.	☐	☐	☐
44		Nagel, Robert , et al.	☐	☐	☐
45		Parzych, James D. , et al.	☐	☐	☐
46		Lawlor, Matthew P. , et al.	☐	☐	☐

	U	1	Document ID	Issue Date	Pages
47	☒	☐	US 5191613 A	19930302	
48	☒	☐	US 5163091 A	19921110	
49	☒	☐	US 5109413 A	19920428	
50	☒	☐	US 5031214 A	19910709	
51	☒	☐	US 4981370 A	19910101	
52	☒	☐	US 4817140 A	19890328	
53	☒	☐	US 4796181 A	19890103	
54	☒	☐	US 4771462 A	19880913	

	Title	Current OR	Current XRef
47	Knowledge based system for document authentication	713/176	340/5.86 ; 705/75 ; 713/186
48	Knowledge based system for document authentication (apparatus)	713/176	340/5.86 ; 713/186
49	Manipulating rights-to-execute in connection with a software copy protection mechanism	705/54	
50	Document authentication apparatus	713/176	713/186
51	Document authentication apparatus	713/176	340/5.86 ; 713/186
52	Software protection system using a single-key cryptosystem, a hardware-based authorization system and a secure coprocessor	705/55	380/277 ; 380/281
53	Billing system for computer software	705/52	380/230 ; 705/32 ; 705/55
54	Communication port encryption/decryption method and apparatus	380/44	713/155 ; 713/162

	Retrieval Classif	Inventor	S	C	P
47		Graziano, James M. , et al.	☐	☐	☐
48		Graziano, James M. , et al.	☐	☐	☐
49		Comerford, Liam D. , et al.	☐	☐	☐
50		Dziewit, Halina S. , et al.	☐	☐	☐
51		Dziewit, Halina S. , et al.	☐	☐	☐
52		Chandra, Ashileshwari N. , et al.	☐	☐	☐
53		Wiedemer, John D.	☐	☐	☐
54		Hannan, Forrest A. , et al.	☐	☐	☐

11/AB/1   (Item 1 from file: 15)

ABSTRACT: Two opposing schools of thought fuel the debate over combating software **piracy** . One camp maintains that anti-**piracy** technologies like encryption are necessary deterrents, while the opposing view holds that any anti- **piracy** technology is useless and that pirates will take their share regardless of the methods used. Publishers are beginning to demand proof that anti-**piracy** technologies work without turning off legitimate users. Instead, what exists so far are descriptions of what today's anti-**piracy** technologies do, how they work, how they are positioned, and how their developers and early adopters see these hardware and software technologies combating the genuine problem of software **piracy** , especially as **piracy** 's prospects grow increasingly intriguing in the lucrative and largely uncharted world of DVD. One way CD replicators are playing a key role in making sure legitimate CDs get into the stores is by applying Source Identification Codes to the discs they press. For software protection, a small amount of code is added to installation files, which works with an added layer of one of several proprietary polymers on the CD-ROM or DVD-ROM media.

11/AB/2   (Item 1 from file: 16)

11/AB/3   (Item 2 from file: 16)

11/AB/4   (Item 1 from file: 148)

11/AB/5   (Item 2 from file: 148)

ABSTRACT: Technological measures such as encryption-based software appear to offer the best protection against software **piracy** on the Internet. Legal remedies are available through litigation, but litigation may not be advantageous under the current system, except against the most egregious pirates. Eventually, technological remedies may be supplemented by legal measures, such as the proposed amendment to the Copyright Act that would prohibit programs and devices that circumvent copyright-protection systems.

11/AB/6   (Item 1 from file: 348)

ABSTRACT EP 959621 A1
    A method for preventing the unauthorised copying of video, comprises: embedding first binary data in video data relating to the luminance of visible portions of plural video frames; embedding second binary data in said video data relating to the luminance of visible portions of plural video frames, said first and second embedding being independent of each other; decoding at least a portion of said embedded binary data; and disabling a recording capability of an associated apparatus in accordance with said decoded data.

11/AB/7   (Item 2 from file: 348)

ABSTRACT EP 959620 A1
    A method of processing video to hide N-bits of embedded information in video data corresponding to visible portions of plural frames thereof, N being at least two, and thereafter producing a pixelated representation

of said processed video data on a display screen, each pixel having a
luminance value, in which method each of plural of said pixels has a
luminance value that is a function of plural bits of said N-bits of
embedded information.

11/AB/8   (Item 3 from file: 348)
DIALOG(R)File 348:(c) 2001 European Patent Office. All rts. reserv.

ABSTRACT EP 681233 A1
    A method and apparatus is provided in a data processing system for
securing access to particular files which are stored in a
computer-accessible memory media. A file management program is provided
as an operating system component of the data processing system. A
plurality of files are stored in a computer-accessible memory media,
including at least one encrypted file and at least one unencrypted file.
For each encrypted file, a preselected portion of the file is recorded in
memory, a decryption block is generated which includes information which
can be utilized to **decrypt** the file, and the decryption block is
incorporated in the file in lieu of the preselected portion which has
been recorded in memory. Then, a file management program is utilized to
monitor data processing system calls for files stored in the
computer-accessible memory media. The file management program determines
whether the called file has an associated decryption block. The called
file is processed in a particular manner dependent upon whether or not
the called file has an associated decryption block. (see image in
original document) (see image in original document)

11/AB/9   (Item 4 from file: 348)
DIALOG(R)File 348:(c) 2001 European Patent Office. All rts. reserv.

ABSTRACT EP 679980 A1
    A method and apparatus is provided for distributing a software object
from a source to a user. A software object is encrypted with an
encryption operation utilizing a long-lived encryption key. It is
directed from the source to the user. It is loaded onto a user-controlled
data processing system having a particular configuration. A numerical
machine identification is derived based at least in part upon the
particular data processing system configuration of the user-controlled
data processing system. A temporary key is derived which is based at
least in part upon the numerical machine identification and the
long-lived encryption key. The long-lived key generator is provided for
receiving the temporary key and producing the long-lived encryption key.
The user is allowed to utilize the temporary key for a prescribed
interval to generate the long-lived encryption key to access the software
object. (see image in original document)

11/AB/10   (Item 5 from file: 348)
DIALOG(R)File 348:(c) 2001 European Patent Office. All rts. reserv.

ABSTRACT EP 679979 A1
    A method and apparatus is provided for distributing software objects
from a producer to a potential user. The software object is reversibly
functionally limited, preferably through encryption, and loaded onto a
computer-accessible memory media along with the file management program.
The computer-accessible memory media is shipped from the producer to the
potential user. The file management program is loaded into a
user-controlled data processing system, and associated with the operating
system for the user-controlled data processing system. The
computer-accessible memory media is read with the user-controlled data
processing system. The file management program is utilized to restrict
access to the software object. (see image in original document)

11/AB/11   (Item 6 from file: 348)
DIALOG(R)File 348:(c) 2001 European Patent Office. All rts. reserv.

ABSTRACT EP 679978 A1

A method and apparatus is provided in a data processing system for securing access to particular files which are stored in a computer-accessible memory media. A file management program is provided as an operating system component of the data processing system. At least one encrypted file and at least one unencrypted file are stored in the computer-accessible memory media. An unencrypted security stub is associated with each of the encrypted files. The security stub is at least partially composed of executable code. The file management program is utilized to monitor data processing calls for a called file stored in the computer-accessible memory media. The file management program determines what the called file has an associated unencrypted security stub. The called file is processed in a particular manner dependent upon whether or not the called file has an associated unencrypted security stub. (see image in original document)

11/AB/12   (Item 7 from file: 348)

ABSTRACT EP 679977 A1

A method and apparatus is provided for transferring encrypted files from a source computer to one or more target computers. An export program is provided in the source computer and an import program is provided in the target computer. The export program decrypts the encrypted file and tags the export operation with an export counter value. The clear text file is then encrypted with an encryption operation utilizing a key which is unique to a transfer memory media, such as diskette serial number. The memory media is carried to a target computer which utilizes the import file to **decrypt** the encrypted file. (see image in original document)

11/AB/13   (Item 8 from file: 348)

ABSTRACT EP 266748 A2

The invention provides a software asset protection mechanism which is based on the separation of the software to be protected from the right to execute that software. Protected software can only be executed on composite computing systems in which a physically and logically secure coprocessor (15) is associated with a host computer (10). The software to be protected is broken down into a protected (encrypted) portion FILE2 EAK and an (optical) unprotected or plain text portion FILE 2 PLAIN. The software is distributed by any conventional software distribution mechanism (for example a floppy disk) including the files already identified along with an encrypted software decryption key FILE1. The coprocessor is capable of decrypting the software decryption key so it can thereafter **decrypt** the software, for execution purposes. However, the coprocessor will not perform these functions unless and until the user's right to execute is evidenced by presentation of a physically secure token (20). The physically secure token provides to the coprocessor token data in plain text form (the physical security or the plain text token data is provided by the cartridge within which token data is stored). The physical properties of that cartridge taken together with the correspondence between the token data provided by the cartridge and the encrypted token data evidence the user's right to execute.

11/AB/14   (Item 9 from file: 348)

ABSTRACT EP 174472 A2

Implementing a shared higher level of privilege on personal computers for copy protection of software.
Method and apparatus which restricts software, distributed on **magnetic media** , to use on a single computing machine (2). The original medium is functionally uncopyable, until it is modified by the execution of a

program stored in a tamper proof co-processor (10) which forms part of
the computing machine. The modified software on the original medium may
then be copied, but the copy is operable only on the computing machine
containing the co-processor that performed the modification.

11/AB/15   (Item 1 from file: 349)

English Abstract
  A field programmable gate array (70) has security configuration features
  to prevent monitoring of the configuration data for the field
  programmable gate array. The configuration data is encrypted by a
  security circuit (64) of the field programmable gate array using a
  security key (62). This encrypted configuration data is stored in an
  external nonvolatile memory (32). To configure the field programmable
  gate array, the encrypted configuration data is decrypted by the security
  circuit (64) of the field programmable gate array using the security key
  stored in the field programmable gate array.

French Abstract
  Un reseau de portes programmable par l'utilisateur (70) presente des
  caracteristiques de configuration de securite empechant le controle des
  donnees de configuration pour le reseau de portes programmable par
  l'utilisateur. Les donnees de configuration sont chiffrees par un circuit
  de securite (64) dudit reseau de portes programmables par l'utilisateur,
  au moyen d'un code de securite (62). Ces donnees de configuration
  chiffrees sont memorisees dans une memoire remanente externe (32). Pour
  la configuration du reseau de portes programmables, les donnees de
  configuration chiffrees sont dechiffrees par le circuit de securite (64)
  dudit reseau de portes, au moyen du code de securite memorise dans ce
  dernier.

11/AB/16   (Item 2 from file: 349)

English Abstract
  A **digital** rights management system for the distribution, protection and
  use of **electronic** content. The system includes a client architecture
  which receives content, where the content is preferably protected by
  encryption and may include a license and individualization features.
  Content is protected at several levels, including: no protection;
  source-sealed; individually-sealed (or "inscribed"); source-signed; and
  fully-individualized (or "owner exclusive"). The client also includes
  and/or receives components which permit the access and protection of the
  encrypted content, as well as components that allow content to be
  provided to the client in a form that is individualized for the client.
  In some cases, access to the content will be governed by a rights
  construct defined in the license bound to the content. The client
  components include an object which accesses encrypted content, an object
  that parses the license and enforces the rights in the license, an object
  which obtains protection software and data that is individualized for the
  client and/or the persona operating the client, and a script of
  instructions that provides individualization information to a distributor
  of content so that the content may be individualized for the client
  and/or its operating persona. Content is generally protected by
  encrypting it with a key and then sealing the key into the content in a
  way that binds it to the meta-data associated with the content. In some
  instances, the key may also be encrypted in such a way as to be
  accessible only be the use of individualized protection software
  installed on the client, thereby binding use of the content to a
  particular client or set of clients.

French Abstract
  L'invention concerne un systeme electronique de gestion de droits
  d'auteur, pour la distribution, la protection et l'utilisation d'un
  contenu electronique. Ce systeme comprend une architecture client qui

recoit le contenu, ce dernier etant de preference protege par un cryptage et pouvant comporter des caracteristiques de licence et d'individualisation. Le contenu peut etre protege a differents niveaux, tels que : absence de protection ; source scellee ; scellement individuel (<= inscrit >=) ; source signee ; et entierement individualise (<= reserve exclusivement au proprietaire >=). Cette architecture client peut egalement comprendre et/ou recevoir des composants permettant d'acceder au contenu crypte et de proteger ce dernier, ainsi que des composants qui permettent de fournir au client un contenu sous une forme individualisee. Dans certains cas, l'acces au contenu est regi par un concept juridique defini dans le licence liee au contenu. Les composants client comprennent un objet qui accede au contenu crypte, un objet qui analyse la licence et fait valoir les droits inclus dans la licence, un objet qui obtient un logiciel et des donnees de protection individualises pour le client et/ou la personne agissant pour le compte du client, ainsi qu'un ensemble d'instructions qui fournit une information d'individualisation a un distributeur de contenu de sorte que le contenu puisse etre individualise pour le client et/ou la personne agissant pour le compte du client. Le contenu est en general protege par cryptage au moyen d'une cle, puis par scellement de cette derniere dans le contenu de sorte qu'elle soit liee aux meta-donnees associees au contenu. Dans certains cas, la cle peut egalement etre cryptee de facon a etre accessible uniquement au moyen d'un logiciel de protection individualise, installe chez le client, l'utilisation du contenu etant alors lie a un client ou a un groupe de clients particuliers.

11/AB/17   (Item 3 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
    A server architecture for a **digital** rights management system that distributes and protects rights in content. The server architecture includes a retail site which sells content items to consumers, a fulfillment site which provides to consumers the content items sold by the retail site, and an activation site which enables consumer reading devices to use content items having an enhanced level of copy protection. Each retail site is equipped with a URL encryption object, which encrypts, according to a secret symmetric key shared between the retail site and the fulfillment site, information that is needed by the fulfillment site to process an order for content sold by the retail site.

French Abstract
    La presente invention concerne une architecture de serveur destinee a un systeme de gestion de droits numeriques qui repartit et protege les droits de contenus. Cette architecture de serveur comprend un site de vente au detail qui vend des articles de contenu a des consommateurs, un site d'execution qui fournit aux consommateurs les articles de contenu vendus par le site de vente au detail, et un site d'activation qui permet aux dispositifs de lecture du consommateur d'utiliser les articles de contenu qui presentent un niveau eleve de protection contre la copie. Chaque site de vente au detail est equipee d'un objet de chiffrage URL, qui chiffre, en fonction d'une cle symetrique secrete partagee entre le site de vente au detail et le site d'execution, les informations requises par le site d'execution pour traiter une commande de contenu vendu par le site de vente au detail.

11/AB/18   (Item 4 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
    A server architecture for a **digital** rights management system that distributes and protects rights in content. The server architecture includes a retail site which sells content items to consumers, a fulfillment site which provides to consumers the content items sold by the retail site, and an activation site which enables consumer reading devices to use content items having an enhanced level of copy protection.

Each retail site is equipped with a URL encryption object, which encrypts, according to a secret symmetric key shared between the retail site and the fulfillment site, information that is needed by the fulfillment site to process an order for content sold by the retail site. Upon selling a content item, the retail site transmits to the purchaser a web page having a link to a URL comprising the address of the fulfillment site and a parameter having the encrypted information. Upon following the link, the fulfillment site downloads the ordered content to the consumer, preparing the content if necessary in accordance with the type of security to be carried with the content. The fulfillment site includes an asynchronous fulfillment pipeline which logs information about processed transactions using a store-and-forward messaging service. The fulfillment site may be implemented as several server devices, each having a cache which stores frequently downloaded content items, in which case the asynchronous fulfillment pipeline may also be used to invalidate the cache if a change is made at one server that affects the cached content items. An activation site provides an activation certificate and a secure repository executable to consumer content-rendering devices which enables those content rendering devices to render content having an enhanced level of copy-resistance. The activation site "activates" client-reading devices in a way that binds them to a persona, and limits the number of devices that may be activated for a particular persona, or the rate at which such devices may be activated for a particular persona.

French Abstract

L'invention concerne une architecture de serveur destinee a un systeme de gestion de droits numerique servant a octroyer et proteger des droits sur un contenu. Cette architecture de serveur comprend un site de vente au detail permettant de vendre des articles de contenu a des consommateurs, un site d'execution fournissant aux consommateurs les articles de contenu vendus par l'intermediaire de ce site de vente au detail, ainsi qu'un site d'activation permettant a des dispositifs de lecture de consommateurs d'utiliser les articles de contenu presentant un niveau eleve de protection contre la copie. Chaque site de vente au detail est muni d'un objet de cryptage URL servant a crypter, selon une cle symetrique secrete partagee entre le site de vente au detail et le site d'execution, des informations requises par le site d'execution pour traiter une commande d'un contenu vendu par l'intermediaire dudit site de vente au detail. Apres la vente d'un article de contenu, le site de vente au detail envoie a l'acheteur une page Web dotee d'un lien vers une adresse URL comprenant l'adresse du site d'execution et un parametre contenant les informations cryptees. Apres l'activation de ce lien, le site d'execution telecharge le contenu commande par le consommateur en preparant ce contenu, si necessaire, selon le type de securite requis pour ledit contenu. Le site d'execution comprend un pipeline d'execution asynchrone qui enregistre des informations sur des transactions effectuees au moyen d'un service de messagerie differee. Ce site d'execution peut etre mis en oeuvre sur plusieurs dispositifs serveurs comprenant chacun une antememoire stockant des articles de contenu frequemment telecharges, auquel cas le pipeline d'execution asynchrone peut egalement servir a invalider l'antememoire si un changement opere au niveau d'un serveur affecte les articles de contenu en antememoire. Un site d'activation fournit un certificat d'activation et un executable de referentiel securise a des dispositifs d'extraction de contenu de consommateurs, les dispositifs d'extraction de contenu pouvant alors extraire les contenus presentant un niveau eleve de resistance a la copie. Ce site d'activation active les dispositifs de lecture clients de maniere a les relier a une personne, et limite le nombre de dispositifs pouvant etre actives pour une personne particuliere ou la vitesse a laquelle ces dispositifs peuvent etre actives pour une personne particuliere.

11/AB/19   **(Item 5 from file: 349)**

English Abstract
  An authorization system (100) and associated method for selectively

authorizing a host system (110) to use one of more items of protected information (115) associated with the host system (110). The authorization system (100) includes a portable authorization device (140) that is removably couplable to the host system (110). The portable authorization device (140) is capable of receiving and storing multiple items of authorization information (171) associated with a plurality of respective items of protected information (115) from one or more information authorities (160, 180, 185). Preferably, the portable authorization device (140) is capable of communicating with multiple types of information authorities (160, 180, 185). The portable authorization device (140) selectively authorizes the host system (110) to use the one or more respective items of protected information (115) based upon the respective authorization information (171) stored therein.

French Abstract
La presente invention concerne un systeme d'autorisation (100) et son procede associe utilises pour autoriser selectivement un systeme hote (110) a utiliser un ou plusieurs elements d'informations protegees (115) associes au systeme hote (110). Ce systeme d'autorisation (100) comprend un dispositif d'autorisation portatif (140) pouvant etre couple de maniere amovible au systeme hote (110). Le dispositif d'autorisation portatif (140) peut recevoir et stocker des elements multiples d'informations d'autorisation (171) associes a plusieurs elements respectifs d'informations protegees (115) d'une ou de plusieurs autorites d'informations (160, 180, 185). De preference, le dispositif d'autorisation portatif (140) peut communiquer avec des types multiples d'autorites d'informations (160, 180, 185). Le dispositif d'autorisation portatif (140) autorise de maniere selective le systeme hote (110) a utiliser les elements respectifs d'informations protegees (115) sur la base des informations d'autorisation respectives (171) qui y sont stockees.

11/AB/20   (Item 6 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
An apparatus and method for decoding of encoded signals representing at least image information from a storage medium is claimed. A storage device (136) is configured to receive the storage medium. A decoder (144) is configured to receive the compressed encrypted encoded signals from the storage medium, and send the signals to a decryptor (320/324). The decryptor (320/324) is configured to **decrypt** the compressed encrypted encoded signals, and send the signals to a decompressor (320/324). The decompressor (320/324) is configured to receive the compressed encoded signals from the decryptor and to decompress the compressed encoded signals to enable display of the image.

French Abstract
Cette invention concerne un dispositif et une technique permettant de decoder a partir d'un support de stockage des signaux codes representant au moins une information image. Un dispositif de stockage (136) est configure pour recevoir un support de stockage. Un decodeur (144) est concu pour recevoir, a partir du support de stockage, des signaux codes cryptes comprimes et de les transmettre a un decrypteur (320/324). Ce decrypteur est concu pour decrypter les signaux codes cryptes compresses et pour les transmettre a un decompresseur (320/324). Ce decompresseur est concu pour recevoir du decrypteur les signaux codes compresses et pour les decompresser en vue de l'affichage de l'image.

11/AB/21   (Item 7 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
An apparatus and method for the encoding and storage of signals representing at least image information onto a storage medium (100) is claimed. A source generator (108) is configured to convert the signals

into digitized image information. A compressor (112) is configured to receive the digitized image information from the source generator (108) and compress the digitized image. An encryptor (112) is configured to receive the compressed digitized image information from the compressor (112) and **encrypt** the compressed digitized image information. A storage device (116) is configured to then store the encrypted compressed digitized image information onto the storage medium.

French Abstract
La presente invention concerne un appareil et un procede de codage et de stockage de signaux qui representent au moins des informations stockees sur un support de stockage (100). Un generateur (108) source est configure de facon a convertir ces signaux en informations d'image numerisee. Un compresseur (112) est configure de facon a recevoir ces informations d'image numerisee en provenance du generateur (108) source et a compresser cette image numerisee. Une machine a chiffrer (112) est configuree de facon a recevoir ces informations d'image numerisee compressee en provenance du compresseur (112) et a chiffrer ces informations d'image numerisee compressee. Un dispositif (116) de stockage est configure de facon a stocker ensuite ces informations d'image numerisee compressee sur le support de stockage.

11/AB/22   (Item 8 from file: 349)

English Abstract
A system, method, and article of manufacture are disclosed that controls the network and manages resources for managing network assets through asset tracking in an e-Commerce-based supply chain framework. Features include automatically caching web content, providing proxy services, managing load balancing such as spreading tasks among servers and rerouting data around problems. The capability to reroute data around problems includes indentifying and automatically bypassing an unavailable network object. Additional features may include a capability to enable remote access and providing integrated firewall services. The remote access capabilities include enabling a high density modem pool and providing a remote access point. The integrated firewall services on the network includes storing and reporting firewall functions and firewall attacks.

French Abstract
L'invention concerne un systeme, un procede, et un article manufacture permettant de commander le reseau et d'en gerer les ressources de maniere a gerer le parc informatique par le suivi des ressources dans un cadre du type chaine d'approvisionnement basee sur le commerce electronique. Parmi les fonctions qu'offre le systeme de l'invention figurent : la mise en memoire cache automatique des contenus Web, l'offre de services proxy, la gestion de l'equilibrage des charges, notamment la repartition des taches entre serveurs et le re-routage des donnees en cas de probleme. Cette fonction de re-routage des donnees en cas de probleme assure l'identification et le contournement automatique d'un objet reseau non disponible. Parmi les autres fonctions, notons la possibilite de permettre un acces a distance et l'offre de services pare-feu integres. Les fonctions d'acces a distance passent par l'activation d'un groupe de modems haute densite et la creation d'un point d'acces a distance. Les services pare-feu integres du reseau gerent le stockage et la signalisation des fonctions pare-feu et des attaques au niveau des pare-feu.

11/AB/23   (Item 9 from file: 349)

English Abstract
A system, method and article of manufacturer are provided for proactive management during maintenance and service in a network-based supply chain environment. Telephone calls, data and other multimedia information are

routed through a network which includes transfer of information across the internet utilizing telephony routing information and internet protocol address information. The network includes a Proactive Threshold Manager which forewarns service providers of an impending breach of contact. The Proactive Threshold Manager sends an alarm to the service provider when the current level of service will miss a service level agreement to maintain a certain level of service.

French Abstract
L'invention concerne un systeme, un procede, et un article manufacture de gestion proactive mis en oeuvre au cours de la maintenance et de l'entretien d'un environnement du type chaine d'approvisionnement reseautee. Les appels telephoniques, les donnees et autres informations multimedia sont routes via un reseau assurant le transfert des informations via Internet au moyen d'informations de routage telephonique et d'informations d'adresse de protocole Internet. Ledit reseau comprend un gestionnaire de seuil proactif qui avertit a l'avance les fournisseurs d'une rupture de contrat imminente. Ledit gestionnaire de seuil proactif envoie une alarme au fournisseur de services lorsque le niveau de service du moment n'atteint plus le niveau de service determine dans le contrat en termes de maintien d'un certain niveau de service.

11/AB/24   (Item 10 from file: 349)

English Abstract
A system, method and article of manufacture are provided for asset management in a network-based supply chain. Utilizing a network, information is received information from at least one service provider. This information includes information relating to present network assets of the service provider. Information is also received utilizing the network from at least one manufacturer. The information from the manufacturers includes information relating to present network assets of the manufacturers. A determination is made for optimal network assets needed for the service provider and manufacturer based on the present network assets of service provider and the manufacturer. Based on this determination, the optimizing of the network assets is managed.

French Abstract
L'invention concerne un systeme, un procede et un article de fabrication destines a la gestion d'actifs dans une chaine d'approvisionnement en reseau. Ce dernier permet de recevoir des informations provenant d'au moins un prestataire de services. Ces informations renferment des elements d'information se rapportant aux actifs actuels en reseau dudit prestataire. Elles sont egalement recues par le biais du reseau en provenance d'au moins un fabricant. Les informations des fabricants comportent des elements d'information se rapportant aux actifs actuels en reseau des fabricants. On determine les actifs en reseau optimaux necessaires au prestataire de services et au fabricant sur la base des actifs actuels en reseau desdits prestataire de services et fabricant. Cette determination permet de gerer l'optimisation des actifs en reseau.

11/AB/25   (Item 11 from file: 349)

English Abstract
A system, method and article of manufacture are provided for collaborative capacity planning during demand and supply planning in a network-based supply chain. Data access is provided from multiple simultaneous data sources utilizing a network for demand and supply planning in a network-based supply chain having at least one service provider and at least one manufacturer. Capacity data is stored utilizing the network.

French Abstract
On decrit un systeme, un procede et un article manufacture qui permettent

d'effectuer la planification en collaboration des capacites lors de la
planification de l'offre et de la demande dans une chaine
d'approvisionnement fondee sur le reseau. L'acces aux donnees provient
d'une pluralite de sources de donnees simultanees auxquelles on accede
par un reseau en vue d'effectuer la planification de l'offre et de la
demande dans une chaine d'approvisionnement fondee sur le reseau
comprenant au moins un fournisseur de service et au moins un fabricant.
Des donnees de capacite sont stockees au moyen du reseau.

11/AB/26   (Item 12 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
A system, method and article of manufacture are provided for affording a
network-based supply chain framework. Installation of a service is
managed utilizing a network. Demand and supply of manufacturer offerings
are planned utilizing the network and orders for the manufacturer
offerings are also managed utilizing the network. The network is also
utilized to manage network assets including providing maintenance and
service for the network assets utilizing the network.

French Abstract
On decrit un systeme, un procede et un article manufacture qui
constituent une structure de chaine d'approvisionnement fondee sur le
reseau. L'installation d'un service est geree au moyen d'un reseau. La
demande et l'approvisionnement des offres de fabricant sont planifies au
moyen du reseau et les commandes relatives aux offres du fabricant sont
egalement gerees au moyen du reseau. Le reseau est egalement utilise pour
gerer les actifs sur le reseau, y compris pour effectuer la maintenance
et le service pour les actifs de reseau au moyen du reseau.

11/AB/27   (Item 13 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
An exhibitor receives encrypted **digital** audiovisual data (103) and
exhibitor authorization data from a distributor. Authorization of the
exhibitor to exhibit the **digital** audiovisual data is ensured by
comparing the exhibitor authorization data to exhibitor provided
identification data. The audiovisual data is decrypted (107) and
exhibited only upon verification of the exhibitor's authorization. The
audiovisual data is watermarked with identifying information (111) so
that pirated analog copies made from the exhibition can be traced to the
source.

French Abstract
Un exploitant recoit des donnees audiovisuelles numeriques (103) ainsi
qu'une autorisation d'exploitation de la part d'un distributeur.
L'autorisation d'exploiter les donnees audiovisuelles numeriques delivree
a l'exploitant est validee par la comparaison des donnees d'autorisation
d'exploitant avec des donnees d'identification fournies par l'exploitant.
Les donnees audiovisuelles sont dechiffrees (107) et exploitees seulement
apres verification de l'autorisation de l'exploitant. Les donnees
audiovisuelles sont marquees d'un filigrane contenant une information
d'identification(111) qui permet de remonter jusqu'a la source des copies
pirate analogiques.

11/AB/28   (Item 14 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
Described herein is audio watermarking technology for inserting and
detecting watermarks in audio signals. The watermark identifies the
content producer, providing a signature that is embedded in the audio
signal and cannot be removed. In one embodiment, a watermarking system

employs chess spread-spectrum sequences to improve the balance of
positive and negative chips in the watermarking sequences. The balance is
not imposed in an orderly fashion, but in a pseudo-random fashion. In
that way, better sequence balance is achieved while preserving its
randomness for an attacker without knowledge of the keys. In another
embodiment, a watermarking system employs an energy-level trigger to
determine whether to skip encoding of a portion of a watermark within a
given time span of an audio clip. If a large discrepancy in energy levels
exists over a given time frame, then the frame is not watermarked, to
avoid audible time-dispersion of artifacts. In another embodiment, a
watermarking system begins encoding of a watermark at a variable position
after the beginning of an audio clip.

French Abstract
    La presente invention concerne une technologie de filigrane numerique
audio permettant d'inserer et de detecter des filigranes dans des signaux
audio tels qu'un clip musical. Le filigrane identifie le producteur de
contenu, fournissant une signature qui est encastree dans le signal audio
et ne peut pas etre retiree. Le filigrane est concu pour survivre a
toutes les sortes habituelles de traitement et d'attaques malveillantes.
Dans l'une des realisations decrites, un systeme de filigrane utilise des
sequences d'echecs a spectre etendu pour ameliorer l'equilibre entre
bribes positives et bribes negatives dans les sequences de filigrane. Cet
equilibre n'est pas impose de facon ordonnee, ce qui peut rendre la
sequence de filigrane plus facile a detecter par un attaquant, mais de
facon pseudo-aleatoire. De cette facon, on obtient un meilleur equilibre
des sequences tout en conservant son caractere aleatoire pour un
attaquant sans connaissance des cles. Selon une autre realisation
decrite, un systeme de filigrane emploie un declencheur a niveau
d'energie pour determiner s'il y a lieu de sauter le codage d'une partie
d'un filigrane dans une duree de temps d'un clip audio. S'il y a un grand
decalage entre niveaux d'energie pendant une trame de temps donnee, c'est
que la trame n'a pas de filigrane, pour eviter une dispersion temporelle
audible des artefacts due aux modifications spectrales (ce qui ressemble
aux effets de pre-echo en codage audio). Dans une autre realisation
decrite, un systeme de filigrane commence a coder un filigrane en une
position variable apres le debut du clip audio.

11/AB/29   **(Item 15 from file: 349)**
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
    Described herein is audio watermarking technology for inserting and
detecting watermarks in audio signals, such as a music clip. The
watermark identifies the content producer, providing a signature that is
embedded in the audio signal and cannot be removed. The watermark is
designed to survive all typical kinds of processing and malicious.
attacks. In one described implementation, a watermarking system employs
cover channel encoder to layer an additional information data message on
top of the watermark. Thus, an informational message is imposed upon the
existing watermark encoded in a signal. In another described
implementation, a watermarking system employs a permutation technique to
further hide the watermark and it may hide the covert message within the
watermark. The order in which data is imposed or encoded is rearranged
based upon a permutation table. The same table is used to reverse permute
the data at the detector.

French Abstract
    L'invention concerne une technique de filigranage numerique audio
consistant a inserer et a detecter des filigranes numeriques dans des
signaux audio, tels qu'un extrait musical. Le filigrane numerique
identifie le producteur de contenu et fournit une signature integree dans
le signal audio qui ne peut pas etre effacee. Ce filigrane est concu pour
survivre a tous les types de traitements et d'attaques malveillantes
classiques. Dans un mode de realisation de l'invention, un systeme de
filigranage numerique fait intervenir un codeur de voie clandestine pour
ajouter un message de donnees d'informations au sommet dudit filigrane.

Ainsi, un message informationnel est impose au filigrane existant code dans un signal. Dans un autre mode de realisation, un systeme de filigranage numerique fait intervenir une technique de permutation pour occulter davantage le filigrane numerique, le message clandestin pouvant ainsi etre dissimule dans ledit filigrane numerique. L'ordre dans lequel les donnees sont imposees ou codees est reorganise sur la base d'une table de permutation. Cette meme table est utilisee pour permuter inversement les donnees au niveau du detecteur.

11/AB/30   (Item 16 from file: 349)

English Abstract
   The present invention is provided for comparison shopping by utilizing a customer's profile to prioritize the features of a group of similar, competing products. First, a customer's profile is developed. This profile may be developed from many sources including customer input, customer buying habits, customer income level, customer searching habits, customer profession, customer education level, customer's purpose of the pending sale, customer's shopping habits, etc. Next, the customer selects multiple, similar items, i.e. products or services to compare. Finally, a comparison table is presented which prioritizes the features in accordance with the customer's profile.

French Abstract
   La presente invention concerne un achat par comparaison grace a l'utilisation d'un profil consommateur pour etablir des priorites dans les caracteristiques d'un groupe de produits analogues en concurrence. D'abord on elabore un profil consommateur. Ce profil peut etre elabore a partir de plusieurs sources, y compris une entree de donnees du consommateur, les habitudes d'achat du consommateur, le revenu du consommateur, les habitudes de recherche du consommateur, la profession du consommateur, le niveau d'education du consommateur, les attentes du consommateur pour la vente en cours, les habitudes d'achat du consommateur, etc. Ensuite, le consommateur selectionne plusieurs articles analogues, c.-a-d. des produits ou des services afin de les comparer. Enfin, un tableau de comparaison produit etablit des priorites de caracteristiques en fonction du profil du consommateur.

11/AB/31   (Item 17 from file: 349)

English Abstract
   A system, method, and article of manufacture are provided that afford a combination of commerce-related web application services. Various features are included such as allowing purchase of products and services via a displayed catalog. As an option, such catalog may be personalized. In various embodiments, a virtual shopping cart environment may be provided. Further, data, i.e. specifications, details, etc., relating to the products and services may be displayed along with a comparison between different products and services. Data relating to needs of a user may also be received for the purpose of outputting a recommendation of the products and services based on the inputted needs. Optionally, features of the products and services may be listed in order to allow the user to configure a specifically tailored product or service. Yet another aspect of the present invention includes outputting an estimate relating to a price and/or availability of the products and services. Further, an order for the products and services may be received after which a tax and a shipping fee are calculated. A status of the delivery of the ordered products and services may also be provided.

French Abstract
   L'invention concerne un systeme, un procede et un article manufacture destines a la fourniture d'une combinaison de services d'application dans le Web lies au commerce. Le systeme presente plusieurs caracteristiques telles que l'achat de produits et de services grace a un catalogue

affiche. En option, ce catalogue peut etre personnalise. Plusieurs modes de realisation peuvent comprendre un environnement de chariot de supermarche virtuel. En outre, des donnees, c.-a-d. des specifications, des details, etc., se rapportant aux produits et services peuvent etre affichees en meme temps qu'une comparaison entre differents produits et services. On peut aussi inclure des donnees relatives aux besoins d'un utilisateur afin de recommander des produits et services donnes sur la base des besoins entres. Eventuellement, on peut etablir une liste des caracteristiques des produits et services afin de permettre a l'utilisateur de configurer un produit ou un service personnalise. Dans un autre aspect de la presente invention, on peut produire une estimation du prix et/ou de la disponibilite des produits et services. En outre, une commande peut etre recue et une taxe et des frais d'expedition calcules. Un etat de l'expedition des produits et services commandes peut egalement etre etabli.

11/AB/32   **(Item 18 from file: 349)**

English Abstract
A system, method, and article of manufacture are provided for prioritizing components of an existing network framework. First, a priority is determined among a plurality of components required for implementation of a predetermined technology using an existing network framework. The existing network framework and the plurality of components are then pictorially represented. Next, a first component of the existing network framework is indicia coded in order to indicate that the first component must be implemented first. Thereafter, a second component and any remaining components of the existing network framework are indicia encoded in order to indicate that the second components and any remaining components must be implemented after the first component.

French Abstract
Cette invention a trait a un systeme, a une methode et a l'article fabrique permettant de classer par ordre de priorite des composants d'une structure de reseau existante. Un certain degre de priorite est, tout d'abord, etabli entre plusieurs composants necessaires a la mise en oeuvre d'une technique predeterminee au moyen d'une structure de reseau existante. Cette derniere ainsi que les composants sont representes graphiquement. Ensuite, un premier composant de la structure de reseau est code sous forme de signe afin d'indiquer qu'il doit etre mis en oeuvre en premier. Un deuxieme composant ainsi que tous les composants restants de la structure de reseau existante sont ensuite codes sous forme de signes afin d'indiquer qu'ils doivent etre mis en oeuvre a la suite du premier.

11/AB/33   **(Item 19 from file: 349)**

English Abstract

French Abstract
La presente invention concerne un systeme permettant de realiser des transactions commerciales virtuelles apres identification des besoins de l'utilisateur. Tout d'abord, le systeme evalue les besoins d'un utilisateur. Il genere ensuite, sur la base des besoins de l'utilisateur, une solution, qui est affichee. Un paiement est alors accepte en echange de la solution. Il convient de noter que dans le cadre du present descriptif de l'invention, ladite solution est, mais pas exclusivement, un produit ou un service.

11/AB/34   **(Item 20 from file: 349)**

English Abstract
   A system, method, and article of manufacture are provided for displaying
phases of delivery of components of a system by first displaying a
pictorial representation of an existing system including a plurality of
components. Next, a first set of components are presented that are to be
delivered in a first phase. This is accomplished by indicia coding the
first set of components in a specific manner. Further, a second set of
components are presented that are to be delivered in a second phase. This
is carried out by indicia coding the second set of components in a manner
unique with respect to the indicia coding of the first set of components.

French Abstract
   L'invention concerne un systeme, un procede et un article manufacture
destines a afficher des phases de fourniture de composants d'un systeme,
en affichant d'abord une representation picturale d'un systeme existant
comprenant plusieurs composants. Ensuite, une premiere serie de
composants a fournir dans une premiere phase est presentee. Cette
operation s'effectue par codage indiciel de la premiere serie de
composants, de facon specifique. Par la suite, une deuxieme serie de
composants a fournir dans une deuxieme phase est presentee. Cette
operation s'effectue par codage indiciel de la deuxieme serie de
composants, de facon unique par rapport au codage indiciel de la premiere
serie de composants.

11/AB/35   **(Item 21 from file: 349)**

English Abstract

French Abstract
   Cette invention se rapporte a un systeme, un procede et un article
manufacture permettant l'acheminement efficace des composants d'un
systeme necessaires a sa mise en pratique. A cet effet, on affiche
d'abord une representation graphique du systeme, qui contient les divers
composants du systeme, puis on code a l'aide d'indices ces composants,
afin d'indiquer lesquels sont necessaires pour la mise en pratique du
systeme.

11/AB/36   **(Item 22 from file: 349)**

English Abstract
   A system, method and article of manufacture are provided for identifying
alliances among a plurality of business entities in components of a
network framework. First, alliances are identified among a plurality of
business entities in terms of components of a current network framework.
Next, a pictorial representation is displayed of the current network
framework and the components. The alliances are then conveyed by indicia
coding the components of the current network framework in which the
alliances exist.

French Abstract
   La presente invention concerne un systeme, un procede et un article de
production permettant d'identifier les alliances au sein d'un groupe de
plusieurs entites commerciales en terme de composants d'un cadre de
reseau. Tout d'abord, les alliances sont identifiees parmi un groupe de
plusieurs entites commerciales en terme de composants d'un cadre de
reseau en cours. Ensuite, une representation graphique du reseau en cours
et des composants est affichee. Les alliances sont alors acheminees en
codant les composants du cadre de reseau en cours dans lequel les
alliances existent avec des marques.

11/AB/37   **(Item 23 from file: 349)**

English Abstract
  Methods and apparatus to enable owners and vendors of software to protect
  intellectual property and to charge per-use. The system produces a unique
  tag for every instance of software. Each user device runs a supervising
  program that ensures, by use of the tag, that no software instance will
  be used infringing on the software owner's rights. When installing or
  using a software instance, the supervising program verifies the
  associated tag and stores the tag. When installing or using untagged
  software, the supervising program fingerprints selected portions of the
  software and stores the fingerprints. A user device's supervising program
  periodically·calls up, or is called up by a guardian center. The guardian
  center detects unauthorized use of software by comparison of current
  call-up data with records of past call-ups. The guardian center completes
  the call-up by enabling or disabling continued use of the monitored
  software instances.

French Abstract
  La presente invention concerne des procedes et appareils permettant a des
  possesseurs et a des vendeurs de logiciel de proteger la propriete
  intellectuelle et d'effectuer un prelevement au moment de l'utilisation.
  Le systeme produit une etiquette unique pour chaque exemplaire de
  logiciel. Chaque dispositif utilisateur execute un programme de
  supervision qui assure, lors de l'utilisation de l'etiquette, qu'aucun
  exemplaire de logiciel ne sera utilise de facon a porter atteinte aux
  droits du possesseur de logiciel. Lors de l'installation ou de
  l'utilisation d'un exemplaire de logiciel, le programme de supervision
  verifie l'etiquette associee et enregistre cette etiquette. Lors de
  l'installation ou de l'utilisation d'un logiciel sans etiquette, le
  programme de supervision releve les empreintes digitales de portions
  choisies du logiciel et enregistre ces empreintes digitales. Un programme
  de supervision du dispositif utilisateur appelle ou est appele, de facon
  periodique, par un centre de garde. Ce centre de garde detecte
  l'utilisation non autorisee de logiciel par comparaison de donnees
  d'appel courantes avec des enregistrements d'appels passes. Ce centre de
  garde acheve l'appel en autorisant ou en empechant la poursuite de
  l'utilisation des exemplaires de logiciel controles.

  11/AB/38   (Item 24 from file: 349)

English Abstract
  A system, method, and article of manufacture is provided for updating
  content stored on a portable storage medium. Upon input of a portable
  storage medium into a machine by a user, the content stored on the
  portable storage medium is read. After reading the content of the
  portable storage medium, a separate storage medium is accessed and
  content is received therefrom. The content from the separate storage
  medium is an update of the content of the portable storage medium. This
  content of the separate storage medium is then displayed.

French Abstract
  L'invention concerne un systeme, un procede, et un article manufacture
  permettant la mise a jour d'un contenu stocke sur un support
  d'enregistrement portable. Des que l'utilisateur introduit le support
  d'enregistrement portable dans un lecteur, le contenu stocke sur ledit
  support d'enregistrement portable est lu. Apres lecture du contenu du
  support d'enregistrement portable, il est possible d'acceder a un support
  d'enregistrement separe, et de recevoir son contenu. Le contenu provenant
  du support d'enregistrement separe est une mise a jour du contenu du
  support d'enregistrement portable. Le contenu de ce support
  d'enregistrement separe est ensuite affiche.

  11/AB/39   (Item 25 from file: 349)

English Abstract
  A system, method, and article of manufacture is provided for tracking the
  distribution of content electronically. First, an **electronic** storage
  medium tracking identifier is incorporated onto an **electronic** storage
  medium and stored on a database. Next, a package tracking identifier is
  situated onto a package in which the **electronic** storage medium is
  stored. The **electronic** storage medium is then tracked while being
  shipped between various entities using the tracking identifier on the
  package. Further, the **electronic** storage medium may be identified using
  the tracking identifier on the **electronic** storage medium in order to
  afford various advertising, security, support, or retail-related
  features.

French Abstract
  L'invention concerne un systeme, un procede et un article de fabrication,
  servant a suivre a la trace la distribution electronique d'un contenu.
  Dans ce systeme, on a d'abord incorpore au support de stockage
  electronique un identificateur permettant de suivre la trace de ce
  support et on a conserve cet identificateur dans une base de donnees.
  Puis, on a place, sur l'emballage du support de stockage electronique, un
  identificateur de poursuite de trace de cet emballage. Ainsi, il est
  possible de suivre la trace de ce support pendant son expedition entre
  diverses entites, a l'aide de l'identificateur place sur l'emballage. En
  outre, il est possible d'identifier le support de stockage electronique a
  l'aide de l'identificateur place sur ce support, ce qui permet l'ajout de
  diverses caracteristiques de publicite, securite, support, ou de
  caracteristiques associees a la vente en detail.

11/AB/40   **(Item 26 from file: 349)**
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
  A system, method, and article of manufacture is provided for tracking and
  supporting the distribution of content electronically. First, an
electronic storage medium tracking identifier is incorporated onto an
electronic storage medium and stored on a database. Next, a package
  tracking identifier is situated onto a package in which the **electronic**
  storage medium is stored. The **electronic** storage medium is then tracked
  while being shipped between various entities using the tracking
  identifier on the package. Further, the **electronic** storage medium may
  be identified using the tracking identifier on the **electronic** storage
  medium in order to afford various advertising, security, support, or
  retail-related features. The system includes logic for downloading and
  updating retailer-specific information of the DVD utilizing BCA
  information for intelligent processing. When a user connects to the
  Internet with a DVD application active, logic detects a live Internet
  connection, reads the BCA information, and initiates a connection to the
  server. Then, the DVD application requests all available support
  information from the server for the retailer of the currently inserted
  DVD. The server performs a table lookup to ascertain the retailer that
  sold the original DVD, and the server performs another table lookup to
  determine the download information, and the server passes the download
  information to the application using HTTP protocol. Finally a transaction
  is posted to the server database that memorializes the events.

French Abstract
  Cette invention se rapporte a un systeme, a un procede et a un article
  produit servant au suivi et a la prise en charge de la distribution d'un
  contenu par voie electronique. Un identificateur de suivi sur support de
  donnees electronique est d'abord incorpore a un support de donnees
  electronique et memorise dans une base de donnees. Un identificateur de
  suivi de paquet est ensuite place sur un paquet dans lequel est stocke le
  support de donnees electronique. Le support de donnees electronique est
  ensuite suivi pendant son expedition entre diverses entites, a l'aide de
  l'identificateur de suivi place sur le paquet. Le support de donnees
  electronique peut en outre etre identifie a l'aide de l'identificateur de
  suivi se trouvant sur le support de donnees electronique, pour permettre

diverses operations de promotion, de securite, de support ou autre
activite de detail. Ce systeme comporte une logique pour le
telechargement et la mise a jour des informations du DVD specifiques au
detaillant, utilisant des informations BCA pour le traitement
intelligent. Lorsqu'un utilisateur se connecte a l'Internet avec une
application DVD active, la logique detecte une connexion Internet en
direct, lit les informations BCA et initialise une connexion avec le
serveur. L'application DVD demande ensuite toutes les informations de
support disponibles aupres du serveur pour le detaillant du DVD en cours
de lecture. Le serveur effectue une consultation de table pour certifier
le detaillant qui a vendu le DVD original, et le serveur effectue une
autre consultation de table pour determiner des informations de
telechargement, et le serveur transmet ces informations de telechargement
a l'application en utilisant un protocole HTTP. Une transaction est
finalement adressee a la base de donnees serveur qui archive l'evenement.

11/AB/41   (Item 27 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
  A system, method, and article of manufacture is provided for tracking the
  distribution of content electronically. First, an **electronic** storage
  medium tracking identifier is incorporated onto an **electronic** storage
  medium and stored on a database. Next, a package tracking identifier is
  situated onto a package in which the **electronic** storage medium is
  stored. The **electronic** storage medium is then tracked while being
  shipped between various entities using the tracking identifier on the
  package. Further, the **electronic** storage medium may be identified using
  the tracking identifier on the **electronic** storage medium in order to
  afford various advertising, security, support, or retail-related
  features.

French Abstract
  Cette invention se rapporte a un systeme, a un procede et a un article
  produit permettant de suivre la distribution d'un contenu par voie
  electronique. Un identificateur de suivi sur support de donnees
  electronique est d'abord incorpore a un support de donnees electronique
  et memorise dans une base de donnees. Un identificateur de suivi de
  paquet est ensuite place sur un paquet, dans lequel est stocke le support
  de donnees electronique. Le support de donnees electronique est ensuite
  suivi pendant son expedition entre diverses entites, a l'aide de
  l'identificateur de suivi place sur le paquet. Le support de donnees
  electronique peut en outre etre identifie a l'aide de l'identificateur de
  suivi se trouvant sur le support de donnees electronique, pour permettre
  diverses operations de publicite, de securite, de support ou autres
  activites de detail.

11/AB/42   (Item 28 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
  A system, method, and article of manufacture is provided for tracking the
  distribution of content electronically. First, an **electronic** storage
  medium tracking identifier is incorporated onto an **electronic** storage
  medium and stored on a database. Next, a package tracking identifier is
  situated onto a package in which the **electronic** storage medium is
  stored. The **electronic** storage medium is then tracked while being
  shipped between various entities using the tracking identifier on the
  package. Further, the **electronic** storage medium may be identified using
  the tracking identifier on the **electronic** storage medium in order to
  afford authorized use of the information contained on the **electronic**
  storage medium.

French Abstract
  Cette invention se rapporte a un systeme, a un procede et a un article
  produit permettant de suivre la distribution d'un contenu par voie

electronique. Un identificateur de suivi sur support de donnees
electronique est d'abord incorpore a un support de donnees electronique
et memorise dans une base de donnees. Un identificateur de suivi de
paquets est ensuite place sur un paquet, dans lequel est stocke le
support de donnees electronique. Le support de donnees electronique est
ensuite suivi pendant son expedition entre diverses entites, a l'aide de
l'identificateur de suivi place sur le paquet. Le support de donnees
electronique peut en outre etre identifie a l'aide de l'identificateur de
suivi se trouvant sur le support de donnees electronique, afin de
permettre l'utilisation autorisee des informations contenues dans le
support de donnees electronique.

11/AB/43   (Item 29 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
   A system, method, and article of manufacture is provided for tracking the
   distribution of content electronically. First, an **electronic** storage
   medium tracking identifier is incorporated onto an **electronic** storage
   medium and stored on a database. Next, a package tracking identifier is
   situated onto a package in which the **electronic** storage medium is
   stored. The **electronic** storage medium is then tracked while being
   shipped between various entities using the tracking identifier on the
   package. Further, the **electronic** storage medium may be identified using
   the tracking identifier on the **electronic** storage medium in order to
   afford authorized purchase and use of the information contained on the
   electronic storage medium.

French Abstract
   Cette invention se rapporte a un systeme, a un procede et a un article
   produit permettant de suivre la distribution d'un contenu par voie
   electronique. Un identificateur de suivi sur support de donnees
   electronique est d'abord incorpore sur un support de donnees electronique
   et memorise dans une base de donnees. Un identificateur de suivi de
   paquet est ensuite place sur un paquet, dans lequel est stocke le support
   de donnees electronique. Le support de donnees electronique est ensuite
   suivi pendant son expedition entre diverses entites, a l'aide de
   l'identificateur de suivi place sur le paquet. Le support de donnees
   electronique peut en outre etre identifie a l'aide de l'identificateur de
   suivi se trouvant sur le support de donnees electronique, pour permettre
   un achat autorise et l'utilisation des informations contenues dans le
   support de donnees electronique.

11/AB/44   (Item 30 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
   A system, method, and article of manufacture is provided for tracking the
   distribution of content electronically. First, an **electronic** storage
   medium tracking identifier is incorporated onto an lectronic storage
   medium and stored on a database. Next, a package tracking identifier is
   situated onto a package in which the **electronic** storage medium is
   stored. The **electronic** storage medium is then tracked while being
   shipped between various entities using the tracking identifier on the
   package. Further, the **electronic** storage medium may be identified using
   the tracking identifier on the lectronic storage medium in order to
   afford authorized use of the information contained on the **electronic**
   storage medium.

French Abstract
   Cette invention se rapporte a un systeme, a un procede et a un article
   produit permettant de suivre la distribution d'un contenu par voie
   electronique. Un identificateur de suivi sur support de donnees
   electronique est d'abord incorpore a un support de donnees electronique
   et memorise dans une base de donnees. Un identificateur de suivi de
   paquet est ensuite place sur un paquet, dans lequel est stocke le support

de donnees electronique. Le support de donnees electronique est ensuite
suivi pendant son expedition entre diverses entites a l'aide de
l'identificateur de suivi place sur le paquet. Le support de donnees
electronique peut en outre etre identifie a l'aide de l'identificateur de
suivi place sur le support de donnees electronique, pour permettre une
utilisation autorisee des informations contenues dans le support de
donnees electronique.

11/AB/45   (Item 31 from file: 349)

English Abstract
  A system, method, and article of manufacture for tracking distribution
  electronically. An **electronic** medium identifier is incorporated onto an
  electronic medium using a Burst Cut Area (BCA). Next, a package
  tracking identifier is located on the package in which the medium is
  stored. The **electronic** medium is tracked during shipment. The system
  includes logic for downloading and updating retailer-specific information
  of the **Digital** Versatile Disk (DVD). When a user connects to the
  Internet with a DVD application (2300), the application reads the BCA
  information. Then, the application requests all downloads from the server
  (2320). The server performs a table lookup to ascertain the retailer of
  the DVD, then performs another table lookup to determine download
  information (2330). The server downloads information to the application
  using HTTP protocol (2340). Finally, the transaction is memorialized in
  the server (2360).

French Abstract
  L'invention concerne un systeme, un procede et un article fabrique, qui
  emploient des moyens electroniques pour localiser une expedition. Un
  identificateur de support electronique est incorpore dans un support
  electronique mettant en oeuvre une zone de decoupage en rafales (BCA).
  Ensuite, un identificateur de localisation de colis est dispose sur le
  colis dans lequel le support est stocke. Le support electronique est
  localise pendant l'expedition. Le systeme comprend une logique qui
  telecharge et met a jour des informations fournies par le detaillant et
  stockees dans le disque numerique polyvalent (DVD). Lorsqu'un utilisateur
  se connecte a Internet au moyen d'une application du DVD (2300),
  l'application lit l'information BCA. Elle demande ensuite tous les
  telechargement emanant du serveur (2320). Le serveur effectue une
  recherche dans une table pour identifier le detaillant du DVD, puis une
  deuxieme recherche pour determiner des informations de telechargement
  (2330). Le serveur telecharge l'information vers l'application au moyen
  d'un protocole HTTP (2340). Enfin, la transaction est memorisee dans le
  serveur (2360).

11/AB/46   (Item 32 from file: 349)

English Abstract
  A device of the same general physical size and shape as a standard audio
  cassette tape, but which accepts **digital** information from any of a
  variety of sources - including for example: Internet transmission, a
  digital computer, or memory cards (especially **digital** memory cards) -
  and plays this **digital** information through any, for example, standard
  audio tape cassette player. The device operates by converting the
  digital representation of the sound into magnetic signals which are
  presented to the read/write head of the cassette player equipment. The
  device allows the user of the cassette player to regulate the audio
  playback using conventional equipment controls such as: START, STOP,
  REWIND, FAST REWIND, FORWARD, FAST FOWARD, etc. The device has the same
  general physical dimensions of a standard audio cassette; at least one
  digital processor; and a slot into which **electronic** media such as, for
  example, memory cards, smart cards having a processor and a memory
  embodied thereon and other memory media may be inserted. Numerous sensors
  detect changes in at least one of the tape equipment mechanisms in the

audio cassette emulator. Various cryptographic techniques are described
for protecting the unauthorized distribution of audio information.

French Abstract
La presente invention concerne un appareil qui presente les memes
caracteristiques generales de dimensions et de forme que la cassette de
magnetophone standard, mais qui est capable, non seulement de prendre en
compte de l'information numerique en provenance de diverses sources
(diffusion par Internet, ordinateur, cartes de memoire de preference
numeriques) mais aussi de restituer l'information numerique notamment via
un lecteur de cassette audio standard. A cet effet, l'appareil prend le
son fourni en format numerique et le convertit en signaux magnetiques
lisibles par la tete de lecture- ecriture du magnetophone a cassette.
L'appareil permet a l'utilisateur du magnetophone a cassette de commander
la restitution audio au moyen des boutons standards (START, STOP, REWIND,
FAST REWIND, FORWARD, FAST FORWARD). Selon une realisation
caracteristique, l'appareil, dont les dimensions physiques generales sont
celles d'une cassette audio standard, comporte au moins un processeur
numerique et une position d'enfichage. On peut installer dans cette
position d'enfichage des supports electroniques (cartes a memoire, cartes
a puce a memoire integree au processeur, et autres supports memoire).
L'emulateur de cassette audio comporte une pluralite de detecteurs qui
decelent tout changement touchant a l'un au moins des mecanismes de
magnetophone. L'invention concerne egalement des techniques
cryptographiques permettant de lutter contre la distribution illicite de
donnees audio.

11/AB/47   (Item 33 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
An automated mailing/shipping system (1, 2, 3) and method communicates an
activation key (90) to a customer terminal (2) for modifying one or more
features of a mailing/shipping program (100) installed at the customer
terminal (2). The modification performed may be the activation,
de-activation, or addition of those features (100). Communication of the
activation key (90) may take place over a computer network such as the
Internet (4), and if so, encryption information may be sent with the key
(70) to protect information exchanges between the customer terminal (2)
and a service provider terminal (1) which sent the key. In accordance
with other aspects of the method, a data base of customer information
maintained at the service provider terminal is searched (200) for
customers (210) who might be interested in receiving a new feature of the
mailing/shipping system (220) or who have pre- purchased a rate table
update service (250). An **electronic** mail message containing the new
feature or rate table is communicated (240) to the customer terminal (2)
for installation and access by the customer.

French Abstract
L'invention concerne un systeme (1, 2, 3) et un procede automatiques
servant a communiquer une cle d'activation (90) a un terminal client (2)
aux fins de modification d'une ou plusieurs caracteristiques d'un
programme de courrier/expedition (100) installe au niveau du terminal
client (2), cette modification pouvant etre une activation, une
desactivation, ou une addition des ces caracteristiques (100). La
communication de la cle d'activation (90) peut s'effectuer sur un reseau
informatique tel que l'Internet (4) et, si tel est le cas, des
informations de cryptage peuvent etre envoyees avec la cle (70) afin de
proteger les echanges d'informations entre le terminal client (2) et le
terminal fournisseur de services (1) qui a envoye la cle. Selon d'autres
aspects du procede, une base de donnees d'informations client, conservee
au niveau du terminal fournisseur de services, est consultee (200) a la
recherche de clients (210) susceptibles d'etre interesses par la
reception d'une nouvelle caracteristique du systeme de
courrier/expedition (220), ou ayant prepaye un service de mise a jour
(250) des tables de tarifs. Un message electronique contenant la nouvelle
caracteristique ou la table de tarifs est communique (240) au terminal

client (2) aux fins d'installation et d'acces par le client.

11/AB/48   (Item 34 from file: 349)

English Abstract
  To enable the source of an unauthorized copy of an information- bearing
  medium, such as a video DVD, to be traced, a compressed **digital** signal
  stream to be stored on the medium is altered to include "running marks",
  that comprise pixel blocks changing in position frame by frame and
  encoded with information designating where and when the copy was made.
  The medium under test is played back synchronously with a reference
  medium containing the locations of the running marks together with
  original video. The source of copying message is advantageously encrypted
  and scrambled to avoid detection or alteration by a copyist. The message
  preferably is spread, for example into a spread spectrum carrier, to
  enhance discrimination among a large number of sources and enable
  demodulation in the presence of noise.

French Abstract
  Afin de remonter a la source d'une copie non autorisee d'un support
  porteur d'informations, tel qu'un DVD video, un train de signaux
  numeriques comprimes a stocker sur le support est modifie pour contenir
  des "marques d'exploitation" contenant des blocs de pixels changeant de
  position trame par trame et codes avec des informations designant ou et
  quand la copie a ete faite. Le support soumis a un test est reproduit de
  facon synchrone avec un support de reference contenant les endroits des
  marques d'exploitation ainsi que la partie video originale. La source du
  message de copie est cryptee et brouillee de facon efficace afin d'eviter
  la detection ou la modification par un plagiaire. Le message est de
  preference etale, par exemple dans un support a spectre etale, afin
  d'ameliorer la distinction parmi un grand nombre de sources et de
  permettre une demodulation en la presence de bruit.

11/AB/49   (Item 35 from file: 349)

English Abstract
  Apparatus and method are provided for the distribution of very high
  quality audio or visual programming material from one or more central
  hubs (102) to one or more presentation locations (56, 104) such as
  theaters using high data rate links such as satellites (106). At the
  central hub (102), a source generation system (108) generates an
  electronic program signal from an analog signal, a
  compression/encryption system (110) codes and digitally encrypts the
  electronic signal, and a modulation/transmission system (114) processes
  the signal for transmission via the satellite (106). A network management
  system (112) at the central hub (102) controls the operation of the hub.
  At the theater (56) or other location, a receiver/demodulator (120)
  receives the programming signal transmitted using the satellite (106). A
  theater management system (122) then controls the storage, routing,
  decoding, and display of the received programming material. Storage
  arrays (124A-124N) in the theater system (104A-104N) provide for
  centralized storage of the programming material. The programming material
  is routed through a local area network to designated auditoriums, several
  of which may operate within a theater system (104A-104N). At each
  auditorium, the programming material is decompressed and decrypted for
  display using **electronic** projection equipment (132A) and standard
  auditorium sound systems (134A).

French Abstract
  L'invention porte sur un appareil et un procede de distribution de
  programmes audio et video de tres haute qualite a partir d'un ou
  plusieurs centraux (102) a destination d'un ou plusieurs sites de
  presentation (56, 104) tels que des theatres a l'aide de liaisons a grand
  debit de donnees, par exemple par satellites (106). Au niveau d'un

central (102), se trouvent: un système source (108) generant le signal electronique de programme a partir d'un signal analogique, un systeme de compression/cryptage (110) codant et cryptant sous forme numerique le signal electronique, un systeme de modulation/emission (114) traitant le signal en vue de sa transmission par satellite (106) ainsi qu'un systeme de gestion du fonctionnement du reseau (112). Au niveau du theatre (56) ou d'un autre site, se trouvent un recepteur/demodulateur (120) recevant le signal transmis par satellite (106), et un systeme de gestion (122) du theatre commandant le stockage, l'acheminement, le decodage et la presentation du programme recu. Les dispositifs de stockage (124A-124N) dudit systeme (104A-104N) assurent le stockage centralise des programmes qui sont achemines par l'intermediaire un reseau local vers differents auditoriums dont plusieurs peuvent fonctionner a l'interieur du systeme (104A-104N) de theatre. Dans chaque auditorium les programmes sont decompresses puis decryptes en vue de leur presentation a l'aide d'equipements electroniques de projection (132A) et de d'equipements acoustiques (134A) classiques pour auditoriums.

11/AB/50   (Item 36 from file: 349)

English Abstract
  A method and concomitant apparatus for compressing (218; 215, 217; 410, 406, 408, 411, 412, 420; 520, 522), multiplexing (219; 216; 440; 524) and, in optional embodiments, encrypting (22), transporting (3), decrypting (42), decompressing (43) and presenting (5) high quality video information in a manner that substantially preserves the fidelity of the video information in a system utilizing standard quality circuits to implement high quality compression, transport and decompression.

French Abstract
  L'invention concerne un procede et un dispositif associe permettant de comprimer (218; 215, 217; 410, 406, 408, 411, 412, 420; 520, 522), de multiplexer (219; 216; 440; 524) et, dans des realisations optionnelles, de chiffrer (22), de transporter (3), de dechiffrer (42), de decomprimer (43) et de presenter (5) des informations video de haute qualite d'une maniere qui conserve sensiblement la fidelite des informations video dans un systeme utilisant des circuits de qualite standard pour mettre en oeuvre une compression, un transport et une decompression de haute qualite.

11/AB/51   (Item 37 from file: 349)

English Abstract
  Embodiments of the present invention provide for the copy protection of distributed material after conditional access is applied, regardless of where the material is distributed. The solutions described provide the advantage of being sufficiently simple in implementation to qualify as "curb high" solutions. "Curb high" solutions provide a range of security from minimal security to a high level of security while requiring relatively fewer system resources to implement than prior approaches.

French Abstract
  Des modes de realisation de l'invention permettent d'assurer une protection contre la copie de materiel diffuse apres application d'un acces conditionnel, quel que soit le lieu de diffusion du materiel. Les solutions proposees offrent l'avantage d'etre suffisamment simples a mettre en oeuvre pour pouvoir etre qualifiees de solutions "haute protection". Ces solutions assurent une gamme de securite allant d'une securite minimale a un haut niveau de securite, tout en necessitant la mise en oeuvre de relativement moins de ressources de systeme par rapport aux approches de la technique anterieure.

11/AB/52   (Item 38 from file: 349)

English Abstract
   The present invention is a method and system universally applicable to
minimize unauthorized use of intellectual property products distributed
to mass market. Identification codes (ID) are assigned to individual
intellectual property product and the means of using such product (User
Means). Process to minimise unauthorized use of such product includes:
firstly, means of selling or distributing such product (Dealer Means) to
generate check code from ID of such product stored in said Dealer Means
and user supplied ID of User Means. Secondly, Dealer Means supplies such
check code to such product placed in said User Means to execute check
code authentication by verifying such check code with the code generated
from ID of such product and ID of said User Means before allowing use of
such product on said User Means to proceed. Alternatively, such check
code is generated by User Means from ID of said User Means and ID of such
product supplied by individual portable tamper-proof data storage device
e.g. plastic card embedded with magnetic storage strip or integrated
circuit, such data storage device being distributed together with such
product to said User Means. Objectives of the present invention are
achieved by embedding essential data and modalities required to execute
such check code generation and check code authentication processes into
at least one tamper-proof data storage device.

French Abstract
   L'invention concerne un procede et un systeme d'application universelle
permettant de reduire au minimum l'utilisation non autorisee d'elements
de propriete intellectuelle diffuses sur le marche de masse. On attribue
des codes d'identification (ID) a ces elements et a leurs systemes
utilisateurs. Le procede comprend les etapes suivantes : etablissement,
par le systeme de vente ou de distribution des elements, d'un code de
verification a partir du code ID de l'element enregistre dans ledit
systeme et du code ID du systeme utilisateur fourni par l'utilisateur,
puis fourniture, par le systeme de vente ou de distribution, du code de
verification a l'element enregistre dans le systeme utilisateur, de
maniere a authentifier ce code en le comparant au code derive du code ID
de l'element correspondant et au code ID du systeme utilisateur, avant
d'autoriser la poursuite de l'utilisation sur ce systeme utilisateur. A
titre de variante, le code de verification est etabli par le systeme
utilisateur a partir du code ID de ce systeme et du code ID de l'element
considere fourni par un dispositif portatif d'enregistrement des donnees
inviolable (par exemple, carte en plastique incorporant une bande
d'enregistrement magnetique ou un circuit integre), ce qui permet de
fournir au systeme utilisateur a la fois le dispositif d'enregistrement
des donnees et l'element lui-meme. On met en oeuvre le procede decrit en
incorporant dans au moins un dispositif d'enregistrement des donnees
inviolable les donnees et les modalites essentielles requises pour
l'etablissement du code de verification et les operations
d'authtification du code en question.

11/AB/53   (Item 39 from file: 349)

English Abstract
   The present invention provides systems and methods for electronic
commerce including secure transaction management and electronic rights
protection. Electronic appliances such as computers employed in
accordance with the present invention help to ensure that information is
accessed and used only in authorized ways, and maintain the integrity,
availability, and/or confidentiality of the information. Secure
subsystems used with such electronic appliances provide a distributed
virtual distribution environment (VDE) that may enforce a secure chain of
handling and control, for example, to control and/or meter or otherwise
monitor use of electronically stored or disseminated information. Such a
virtual distribution environment may be used to protect rights of various
participants in electronic commerce and other electronic or
electronic-facilitated transactions. Secure distributed and other

operating system environments and architectures, employing, for example, secure semiconductor processing arrangements that may establish secure, protected environments at each node. These techniques may be used to support an end-to-end electronic information distribution capability that may be used, for example, utilizing the "electronic highway".

French Abstract
La presente invention concerne des systemes et des procedes de commerce electronique comprenant une gestion de transactions securisees et la protection de droits electroniques. Des appareils electroniques tels que des ordinateurs utilises conformement a la presente invention contribuent a assurer que l'acces aux informations et l'utilisation des informations ne se font que par des voies autorisees et ils maintiennent l'integrite, la disponibilite et/ou la confidentialite des informations. Des sous-systemes securises utilises avec ces appareils electroniques constituent un environnement de distribution virtuel (VDE) reparti pouvant faire valoir une chaine securisee de traitement et de commande, par exemple, pour commander et/ou mesurer ou encore controler l'utilisation d'informations memorisees ou disseminees electroniquement. Cet environnement de distribution virtuel peut etre utilise pour proteger les droits de divers participants dans le commerce electronique et dans d'autres transactions electroniques ou dans lesquelles intervient l'electronique. Des environnements et des architectures de systemes repartis securises et autres systemes d'exploitation emploient, par exemple, des arrangements de traitement a semi-conducteurs securises pouvant etablir des environnments proteges securises a chaque noeud. On peut utiliser ces techniques pour apporter un soutien a une capacite de distribution d'informations electroniques de bout-en-bout pouvant etre utilisees, par exemple, en empruntant l'"autoroute electronique".

11/AB/54   (Item 40 from file: 349)

English Abstract
A rights management arrangement for storage media such as optical **digital** video disks (DVDs, also called **digital** versatile disks) provides adequate copy protection in a limited, inexpensive mass­produceable, low­capability platform such as a dedicated home consumer disk player and also provides enhanced, more flexible security techniques and methods when the same media are used with platforms having higher security capabilities. A control object (or set) defines plural rights management rules for instance, price for performance or rules governing redistribution. Low capability platforms may enable only a subset of the control rules such as controls on copying or marking of played material. Higher capability platforms may enable all (or different subsets) of the rules. Cryptographically strong security is provided by encrypting at least some of the information carried by the media and enabling decryption based on the control set and/or other limitations. A secure "software container" can be used to protectively encapsulate (e.g., by cryptographic techniques) various **digital** property content (e.g., audio, video, game, etc.) and control object (i.e., set of rules) information. A standardized container format is provided for general use on/with various mediums and platforms. In addition, a special purpose container may be provided for DVD medium and appliances (e.g., recorders, players, etc.) that contains DVD program content (**digital** property) and DVD medium specific rules. The techniques, systems and methods disclosed herein are capable of achieving compatibility with other protection standards, such as for example, CGMA and Matsushita data protection standards adopted for DVDs. Cooperative rights management may also be provided, where plural networked rights management arrangements collectively control a rights management event on one or more of such arrangements.

French Abstract
Ce dispositif de gestion des droits pour les supports de stockage tels que videodisques optiques numeriques (egalement appeles disques numeriques multifonctions) assure une protection anti­piratage

efficace en utilisation avec une unite limitee, produite en masse, de
cout modique, a faible capacite telle qu'un lecteur de disque de
particulier et applique des techniques et des procedes perfectionnes,
plus souples, lorsque les memes supports sont utilises avec des unites
presentant des capacites superieures en matiere de securite. Un module ou
ensemble de commande definit des regles de gestion de droits multiples,
par exemple, un paiement par operation de lecture ou des regles de
redistribution. Les unites a faible capacite peuvent permettre seulement
l'application d'un sous­ensemble de regles de commande, portant par
exemple sur la copie ou le marquage du materiel utilise. Des unites a
capacite superieure peuvent permettre l'application de l'ensemble des
regles, ou d'autres sous­ensembles de regles. Une securite de niveau
cryptographique est assuree par le chiffrement d'au moins une partie des
informations portees par le support, le dechiffrement se faisant a l'aide
de l'ensemble de commande et/ou d'autres elements. Une "boite a logiciel"
securisee peut etre utilisee pour enfermer et proteger (par exemple, par
des techniques cryptographiques) diverses informations sur le contenu
numerique (par exemple, audio, video, jeux, etc.) et l'unite de commande
(ensemble de regles). Une configuration de boite uniformisee est utilisee
de facon generale avec differents supports et unites. De plus, une boite
specialisee peut etre ajoutee pour les supports et accessoires
videodisques (par exemple enregistreurs, lecteurs, etc.) contenant des
programmes videodisques (contenu numerique) et des regles specifiques au
support videodisque. Les techniques, systemes et procedes decrits peuvent
etre compatibles avec d'autres normes de protection telles que, par
exemple, les normes de protection CGMA et Matsushita adoptees pour les
videodisques. Il peut y avoir une gestion des droits cooperative,
plusieurs dispositifs de gestion de droits mis en reseau regulant
collectivement une operation de gestion des droits sur un ou plusieurs
dispositifs.

11/AB/55   (Item 41 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
  Various improvements to steganographic systems, and applications
  therefore, are disclosed. The improvements include facilitating scale and
  rotation registration for steganographic decoding by use of rotationally
  symmetric steganographically embedded patterns and subliminal **digital**
  graticules; improved techniques for decoding without access to unencoded
  originals; improving robustness of steganographic coding in motion
  pictures and/or in the presence of lossy compression/decompression; and
  representing data (1690) by patterned bit cells (802) whose energy in the
  spatial domain facilitates decoding registration (1692). Applications
  include enhanced­security financial transactions, counterfeit
  resistant identification cards, fraud deterrent systems for cellular
  telephony, covert modem channels in video transmissions, photo
  duplication kiosks with automatic copyright detection, and hotlinked
  image objects (e.g., with embedded URLs) for use on the Internet.

French Abstract
  L'invention decrit diverses ameliorations de systemes steganographiques
  et d'applications desdits systemes. Ces ameliorations sont destinees a
  faciliter un reperage d'echelle et de rotation pour le decodage
  steganographique en utilisant des schemas a symetrie de revolution
  integres selon des principes steganographiques et des canevas numeriques
  subliminaux. Les ameliorations consistent egalement a fournir des
  techniques ameliorees permettant des decodages sans acceder a des
  originaux non codes, d'obtenir une plus grande fiabilite du codage
  steganographique dans des images animees et/ou lors de
  compression/decompression avec beaucoup de pertes. Les ameliorations
  consistent en outre a realiser une representation de donnees (1690)
  utilisant des cellules a profil binaire (802) dont l'energie dans le
  domaine spatial facilite l'alignement du decodage (1692). Des
  applications de l'invention permettent d'ameliorer la securite de
  transactions financieres, de rendre plus difficile la falsification de
  cartes d'identification, de creer des systemes qui decouragent la

contrefacon en telephonie cellulaire, d'effectuer des transmissions video
en utilisant des canaux de modem caches, d'equiper des kiosques de
reproduction de photos de dispositif de detection automatique de
copyright et de disposer d'objets d'images dotes de liens dynamiques
(integrant, par exemple, des localisateurs de ressources uniformes)
utilisables sur Internet.

11/AB/56   (Item 42 from file: 349)

English Abstract
A laser microinscribing system includes a Q-switched Nd: YLF laser (1)
with a harmonic converter producing an output of about 530 nm, an optical
system including a focussing lens, a gemstone mounting holder (144) that
is displaceable along three axes for moving a workpiece (11) such as a
gemstone with respect to the optical system so that laser energy is
presented to desired positions, an imaging system for viewing the
gemstone from a plurality of viewpoints including a top CCD (28) and a
side CCD (32), a processor controlling the position of the holder (144)
based on marking instructions and a predetermined program, and a storage
system (156) for storing information relating to images of a plurality of
workpieces. A rigid frame supports the laser (1), the optical system and
the holder (144) to increase immunity to vibrational misalignments. A
secure certificate of authenticity of a marked workpiece (11) is
preferably provided having an image of the marking as well as the outline
of a girdle of the gemstone.

Japanese Abstract
L'invention concerne un systeme de micromarquage par energie laser
comprenant: un laser Nd:YLF a impulsions geantes (1) avec un
convertisseur harmonique produisant un signal d'une longueur d'onde de
530 nm environ; un systeme optique pourvu d'une lentille de focalisation;
un support de pierre precieuse (144) pouvant etre mu le long de trois
axes pour deplacer une piece a marquer (11), telle qu'une pierre
precieuse, par rapport au systeme optique, de sorte que l'energie laser
vienne frapper des emplacements desires; un systeme d'imagerie permettant
d'observer la pierre precieuse depuis une pluralite de points avantageux
et comprenant un capteur a CCD superieur (28) et un capteur a CCD lateral
(32); un processeur commandant la position du support (144) sur la base
d'instructions de marquage et d'un programme predetermine; et un systeme
de memoire (156) servant au stockage d'informations relatives aux images
d'une pluralite de pieces. Un chassis rigide soutient le laser (1), le
systeme optique et le support (144) pour empecher encore plus les
desalignements dus aux vibrations. Un certificat sur d'authenticite
concernant une piece marquee (11) est de preference fourni avec une image
montrant les marques ainsi que le contour de la rondiste de la pierre
precieuse.

11/AB/57   (Item 43 from file: 349)

English Abstract
Various improvements to steganographic systems, and applications
therefore, are disclosed. The improvements include facilitating scale and
rotation registration for steganographic decoding by use of rotationally
symmetric steganographically embedded patterns and subliminal **digital**
graticules; improved techniques for decoding without access to unencoded
originals; improving robustness of steganographic coding in motion
pictures and/or in the presence of lossy compression/decompression; and
representing data by patterned bit cells whose energy in the spatial
domain facilitates decoding registration. Applications include
enhanced-security financial transactions, counterfeit resistant
identification cards, fraud deterrent systems for cellular telephony,
covert modem channels in video transmission, photo duplication kiosks
with automatic copyright detection, and hotlinked image objects (e.g.
with embedded URLs) for use on the internet.

Japanese Abstract
  L'invention a pour objet diverses ameliorations et applications dans le
  domaine de la steganographie. Ces ameliorations consistent a faciliter la
  mise a l'echelle et l'enregistrement de la rotation, pour le decodage
  steganographique, a l'aide de motifs encastres de maniere
  steganographique, symetriques en rotation, et de graticules numeriques
  subliminaux. Ces ameliorations consistent aussi en techniques ameliorees
  de decodage sans acces aux originaux non codes; Elles consistent
  egalement a ameliorer la resistance du codage steganographique dans les
  images en mouvement et/ou en presence de compression/decompression a
  pertes; et a representer les donnees par des configurations de cellules
  binaires dont l'energie dans le domaine spatial facilite l'enregistrement
  du decodage. Les applications comprennent l'amelioration de la securite
  des transactions financieres, des cartes d'identification resistant aux
  contrefacons, des systemes de protection contre les fraudes pour la
  telephonie cellulaire, des canaux de modem secrets dans les transmissions
  video, des kiosques de reproduction de photos a systeme de detection
  automatique de droits d'auteurs, et des objets images a liaison
  electronique (par exemple, avec des localisateurs URL encastres) destines
  a etre utilises sur Internet.

11/AB/58   (Item 44 from file: 349)

English Abstract
  The present invention provides systems and methods for electronic
  commerce including secure transaction management and electronic rights
  protection. Electronic appliances such as computers employed in
  accordance with the present invention help to ensure that information is
  accessed and used only in authorized ways, and maintain the integrity,
  availability, and/or confidentiality of the information. Secure
  subsystems used with such electronic appliances provide a distributed
  virtual distribution environment (VDE) that may enforce a secure chain of
  handling and control, for example, to control and/or meter or otherwise
  monitor use of electronically stored or disseminated information. Such a
  virtual distribution environment may be used to protect rights of various
  participants in electronic commerce and other electronic or
  electronic-facilitated transactions. Secure distributed and other
  operating system environments and architectures, employing, for example,
  secure semiconductor processing arrangements that may establish secure,
  protected environments at each node. These techniques may be used to
  support an end-to-end electronic information distribution capability that
  may be used, for example, utilizing the "electronic highway".

Japanese Abstract
  Systemes et procedes destines au domaine du commerce electronique, et
  notamment a la gestion securisee des transactions et a la protection
  electronique des droits. Les appareils electroniques tels que les
  ordinateurs utilises conformement a la presente invention permettent
  d'assurer que les informations ne sont consultees et exploitees que de
  maniere autorisee, et ils conservent l'integrite, la disponibilite et/ou
  le caractere confidentiel des informations. Les sous-systemes securises
  utilises en association avec de tels appareils electroniques constituent
  un environnement de distribution virtuel distribue (VDE) apte a imposer
  une chaine securisee de traitement et de commande, par exemple pour la
  commande et/ou la mesure ou encore le controle de l'utilisation
  d'informations stockees ou diffusees electroniquement. Cet environnement
  de distribution virtuel peut servir a proteger les droits de differents
  individus impliques dans le commerce electronique et dans d'autres
  transactions electroniques ou assistees par des moyens electroniques. On
  a egalement prevu des environnements et architectures de systeme
  d'exploitation distribues, securises et autres mettant en oeuvre, par
  exemple, des ensembles de traitement securise a semi-conducteurs pouvant
  etablir des environnements securises et proteges au niveau de chaque
  noeud. Ces techniques peuvent servir de soutien pour une fonction
  electronique de distribution d'informations de bout en bout, cette

fonction etant utilisable, par exemple, dans le domaine de l'"autoroute
electronique".

11/AB/59   (Item 45 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
   A method for preventing use of software on an unauthorized computer. The
   software is programmed to **encrypt** and output to the user a validation
   number derived from information received by the software from the
   computer of one or more computer characteristics providing an
   unchangeable and unique computer identification. A second computer is
   operated for the software vendor to **encrypt** an activation number
   derived from the validation number and supplied to the user for input to
   the user's computer. The activation number includes one or more randomly-
   generated digits which, when a predetermined mathematical operation is
   performed thereon and on at least one of the digits of the validation
   number, yields a derived balance number. A preselected signature and
   other information is randomly scattered among randomly generated bytes
   along with a product identification number as a thumbprint/productprint
   which is encrypted by the balance number derived by the user's computer
   from the validation and activation numbers and which is on the hard disk
   drive of the user's computer. The software is authorized for use in the
   user's computer if the preselected signature is retrieved after the
   predetermined balance number is applied to **decrypt** the information
   including the preselected signature.
Japanese Abstract
   L'invention concerne un procede pour empecher l'utilisation d'un logiciel
   sur un ordinateur non autorise. Le logiciel est programme pour coder et
   fournir a l'utilisateur un nombre de validation derive des informations
   recues par le logiciel depuis l'ordinateur, concernant une ou plusieurs
   caracteristiques de l'ordinateur assurant une identification permanente
   et univoque de l'ordinateur. Le vendeur du logiciel utilise un second
   ordinateur pour coder un nombre d'activation derive du nombre de
   validation et fourni a l'utilisateur pour l'entrer dans son ordinateur.
   Le nombre d'activation comporte un ou plusieurs chiffres generes de
   maniere aleatoire. Lorsqu'on effectue une operation mathematique
   predeterminee sur ce chiffre ou ces chiffres et sur au moins un des
   chiffres du nombre de validation, on obtient un nombre derive residuel.
   Une signature preselectionnee et d'autres informations sont eparpillees
   d'une maniere aleatoire parmi les bits produits de maniere aleatoire en
   meme temps que le nombre d'identification du produit pour constituer une
   empreinte digitale/empreinte produit qui est codee par le nombre residuel
   derive par l'ordinateur de l'utilisateur a partir des nombres de
   validation et d'activation et qui se trouve dans l'unite de disque dur de
   l'ordinateur de l'utilisateur. Le logiciel peut etre utilise dans
   l'ordinateur de l'utilisateur si on recupere la signature preselectionnee
   apres que le nombre residuel predetermine a ete applique pour decoder les
   informations comprenant la signature preselectionnee.

11/AB/60   (Item 46 from file: 349)
DIALOG(R)File 349:(c) 2001 WIPO/MicroPat. All rts. reserv.

English Abstract
   An identification code signal is impressed on a carrier to be identified
   (such as an **electronic** data signal or a physical medium) in a manner
   that permits the identification signal later to be discerned and the
   carrier thereby identified. The method and apparatus are characterized by
   robustness despite degradation of the encoded carrier, and by holographic
   permeation of the identification signal throughout the carrier. An
   exemplary embodiment is a processor that embeds the identification signal
   onto a carrier signal in real time.

Japanese Abstract
   Un signal de code d'identification est imprime sur un support destine a
   etre identifie (tel qu'un signal de donnees electronique ou un support

physique) de sorte que le signal d'identification puisse etre reconnu par
la suite et que le support puisse etre identifie. Lesdits procede et
appareil se caracterisent par leur robustesse en depit de la
deterioration du support code, et par une penetration holographique du
signal d'identification dans le support. Dans un mode de realisation cite
en exemple, un processeur integre le signal d'identification sur un
signal porteur en temps reel.

11/AB/61   (Item 1 from file: 647)
DIALOG(R)File 647:(c) 2001 CMP. All rts. reserv.

TEXT:
     Las Vegas, Nev. - On the eve of the Winter Consumer Electronics Show
here, N.V. Philips last week challenged **digital** audio tape with a new
digital cassette system that can also play billions of analog cassette
tapes already in the field.

11/AB/62   (Item 1 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

An input content signal--representing audio, or video--is encoded to hide
plural-bit auxiliary data therein. The process generates an intermediate
signal that is a function of (a) the plural-bit auxiliary data, and (b)
data related to human perception attributes of the content signal. This
intermediate signal is then summed with the content signal to effect
encoding. The plural-bit auxiliary data can include copy control data,
i.e., data that can be sensed by a consumer **electronic** device and used to
disable a copying operation. The intermediate signal may include a
pseudorandom key signal so as to obscure the encoding and require knowledge
of a corresponding key at the decoder to extract the auxiliary data from
the encoded content. In some embodiments, calibration data is encoded in
the content signal with the auxiliary data. This calibration data desirably
has known properties (e.g., spectral attributes, data content, etc.)
facilitating its identification in the encoded content signal. The encoding
is desirably robust against various forms of content degradation, e.g.,
lossy compression/decompression, scaling, resampling, conversion from
 digital to analog and back again, etc., so that the auxiliary data can be
detected from the content notwithstanding such corruption.

11/AB/63   (Item 2 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

The present invention provides systems and methods for secure transaction
management and electronic rights protection. Electronic appliances such as
computers equipped in accordance with the present invention help to ensure
that information is accessed and used only in authorized ways, and maintain
the integrity, availability, and/or confidentiality of the information.
Such electronic appliances provide a distributed virtual distribution
environment (VDE) that may enforce a secure chain of handling and control,
for example, to control and/or meter or otherwise monitor use of
electronically stored or disseminated information. Such a virtual
distribution environment may be used to protect rights of various
participants in electronic commerce and other electronic or
electronic-facilitated transactions. Distributed and other operating
systems, environments and architectures, such as, for example, those using
tamper-resistant hardware-based processors, may establish security at each
node. These techniques may be used to support an all-electronic information
distribution, for example, utilizing the "electronic highway."

11/AB/64   (Item 3 from file: 654)

ABSTRACT

A reproduction apparatus includes a lens for imaging a customer-provided original onto an opto-**electronic** detector for producing image data, and a reproduction system for producing a copy therefrom. The apparatus further includes a detector for sensing data steganographically-encoded information in the image data, and for interrupting the copying process if such data is detected.

11/AB/65   (Item 4 from file: 654)

ABSTRACT

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

11/AB/66   (Item 5 from file: 654)

ABSTRACT

A laser energy microinscribing system, comprising a semiconductor excited Q-switched solid state laser energy source; a cut gemstone mounting system, allowing optical access to a mounted workpiece; an optical system for focusing laser energy from the laser energy source onto a cut gemstone; a displaceable stage for moving said gemstone mounting system with respect to said optical system so that said focused laser energy is presented to desired positions on said gemstone, having a control input; an imaging system for viewing the gemstone from a plurality of vantage points; and a rigid frame supporting said laser, said optical system and said stage in fixed relation, to resist differential movements of said laser, said optical system and said stage and increase immunity to vibrational misalignments. The laser energy source is preferably a semiconductor diode excited Q-switched Nd:YLF laser with a harmonic converter having an output of about 530 nm. The system may further comprise an input for receiving marking instructions; a processor for controlling said displaceable stage based on said marking instructions and said imaging system, to selectively generate a marking based on said instructions and a predetermined program; and a storage system for electronically storing information relating to images of a plurality of workpieces. A secure certificate of authenticity of a marked workpiece is also provided.

11/AB/67   (Item 6 from file: 654)

ABSTRACT

A software licensing system includes a license generator located at a
licensing clearinghouse and at least one license server and multiple
clients located at a company or entity. When a company wants a software
license, it sends a purchase request (and appropriate fee) to the licensing
clearinghouse. The license generator at the clearinghouse creates a license
pack containing a set of one or more individual software licenses. To
prevent the license pack from being copied and installed on multiple
license servers, the license generator assigns a unique license pack ID to
the license pack and associates the license pack ID with the particular
license server in a master license database kept at the licensing
clearinghouse. The license generator digitally signs the license pack and
encrypts it with the license server's public key. The license server is
responsible for distributing the software licenses from the license pack to
individual clients. When a client needs a license, the license server
determines the client's operating system platform and grants the
appropriate license. To prevent an issued license from being copied from
one client machine to another, the software license is assigned to a
specific client by including a client ID within the license. The software
license also has a license ID that is associated with the client ID in a
database record kept at the license server. The license server digitally
signs the software license and encrypts it using the client's public key.
The license is stored locally at the client.

11/AB/68   (Item 7 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

Documents and other items can be delivered electronically from sender to
recipient with a level of trustedness approaching or exceeding that
provided by a personal document courier. A trusted·**electronic** go-between
can validate, witness and/or archive transactions while, in some cases,
actively participating in or directing the transaction.. Printed or imaged
documents can be marked using handwritten signature images, seal images,
electronic fingerprinting, watermarking, and/or steganography.
Electronic commercial transactions and transmissions take place in a
reliable, "trusted" virtual distribution environment that provides
significant efficiency and cost savings benefits to users in addition to
providing an extremely high degree of confidence and trustedness. The
systems and techniques have many uses including but not limited to secure
document delivery, execution of legal documents, and **electronic** data
interchange (EDI).

11/AB/69   (Item 8 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

Secure computation environments are protected from bogus or rogue load
modules, executables and other data elements through use of **digital**
signatures, seals and certificates issued by a verifying authority. A
verifying authority--which may be a trusted independent third party--tests
the load modules or other executables to verify that their corresponding
specifications are accurate and complete, and then digitally signs the load
module or other executable based on tamper resistance work factor
classification. Secure computation environments with different tamper
resistance work factors use different verification **digital** signature
authentication techniques (e.g., different signature algorithms and/or
signature verification keys)--allowing one tamper resistance work factor
environment to protect itself against load modules from another, different
tamper resistance work factor environment. Several dissimilar **digital**
signature algorithms may be used to reduce vulnerability from algorithm
compromise, and subsets of multiple **digital** signatures may be used to

reduce the scope of any specific compromise.

11/AB/70   (Item 9 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

Various improvements to steganographic systems, and applications therefore,
are disclosed. The improvements include facilitating scale and rotation
registration for steganographic decoding by use of rotationally symmetric
steganographically embedded patterns and subliminal **digital** graticules;
improved techniques for decoding without access to unencoded originals;
improving robustness of steganographic coding in motion pictures and/or in
the presence of lossy compression/decompression; and representing data by
patterned bit cells whose energy in the spatial domain facilitates decoding
registration. Applications include enhanced-security financial
transactions, counterfeit resistant identification cards, fraud deterrent
systems for cellular telephony, covert modem channels in video
transmissions, photo duplication kiosks with automatic copyright detection,
and hotlinked image objects (e.g. with embedded URLs) for use on the
internet.

11/AB/71   (Item 10 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

Technology is now available permitting consumers to make amateur- or even
professional-grade copies of photographs. For wedding and portrait
photographers, in particular, the business of making duplications is
fundamental to their livelihoods. The threat of such copying is felt
strongly. To redress these concerns, a machine-readable marking is provided
on emulsion films, photographic papers, and the like. The marking encodes
digital information, yet is essentially imperceptible to the human eye. A
photographic duplication kiosk can be constructed to read this embedded
information and, if warranted by the embedded information, to disable the
kiosk's copying function. An exemplary embodiment pre-exposes the
photographic product with a spatial domain representation of the embedded
data, and may include rotationally symmetric one- or two-dimensional
patterns. Numerous other implementations are similarly practical."

11/AB/72   (Item 11 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

An information processing system including an encryption processing logic
module and a decryption processing logic module for enabling the encryption
of **digital** information to be decrypted with a decryption key K. The
encryption processing module includes logic for encrypting the **digital**
information, distributing the **digital** information and authorizing a user
to **decrypt** the information. The decryption processing module includes
logic for the user to communicate a user number n sub i to receive an
authorization number a sub i from the authorization logic in the encryption
processing module and extrication logic for extricating the decryption key.
The user number n sub i uniquely identifies, and is valuable to, the user,
so valuable in fact that the user would be unwilling to publically dislcose
it. The extrication logic operates on a **digital** signet pair (a sub i, n
sub i) consisting of the authorization number and user number, to extract
K. The decryption logic then uses K to make the content available to the
user. The extrication function is fully available to the user as a
publicly-computable function in which it is computationally infeasible to
use the extrication function to determine other valid **digital** signet
pairs which can be used to extract K.

ABSTRACT

An identification code signal is hidden in a carrier signal (such as an
electronic data signal or a physical medium) in a manner that permits the
identification signal later to be discerned. The carrier signal can thereby
be identified, or some machine responsive action can thereby be taken. The
technique can be applied in video imagery embodiments to control associated
video equipment, e.g. to serve as a copy control signal.

ABSTRACT

The present invention provides systems and methods for secure transaction
management and electronic rights protection. Electronic appliances such as
computers equipped in accordance with the present invention help to ensure
that information is accessed and used only in authorized ways, and maintain
the integrity, availability, and/or confidentiality of the information.
Such electronic appliances provide a distributed virtual distribution
environment (VDE) that may enforce a secure chain of handling and control,
for example, to control and/or meter or otherwise monitor use of
electronically stored or disseminated information. Such a virtual
distribution environment may be used to protect rights of various
participants in electronic commerce and other electronic or
electronic-facilitated transactions. Distributed and other operating
systems, environments and architectures, such as, for example, those using
tamper-resistant hardware-based processors, may establish security at each
node. These techniques may be used to support an all-electronic information
distribution, for example, utilizing the "electronic highway."

ABSTRACT

An information processing system including an encryption processing logic
module and a decryption processing logic module for enabling the encryption
of **digital** information to be decrypted with a decryption key K. The
encryption processing module includes logic for encrypting the **digital**
information, distributing the **digital** information and authorizing a user
to **decrypt** the information. The decryption processing module includes
logic for the user to communicate a user number n sub i to receive an
authorization number a sub i (a sub i being calculated as equal to ((K sym
n sub i) raised to the power of (1/n sub i ' mod phi from the authorization
logic in the encryption processing module and extrication logic for
extricating the decryption key. The user number n sub i uniquely
identifies, and is valuable to, the user, so valuable in fact that the user
would be unwilling to publically disclose it. The extrication logic
operates on a **digital** signet pair (a sub i, n sub i) consisting of the
authorization number and user number, to extract K (K being calculated as
equal to ((a sub i raised to the power of n sub i ') mod N sym n sub i)).
The decryption logic then uses K to make the content available to the
user. The extrication function is fully available to the user as a
publicly-computable function in which it is computationally infeasible to
use the extrication function to determine other valid **digital** signet
pairs which can be used to extract K.

ABSTRACT

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

11/AB/77   (Item 16 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

Software is distributed without entitlement to run, while a separately distributed encrypted entitlement key enables execution of the software. The key includes the serial number of the computer for which the software is licensed, together with a plurality of entitlement bits indicating which software modules are entitled to run on the machine. A secure decryption mechanism contained on the computer fetches its serial number and uses it as a key to **decrypt** the entitlement information, which is then stored in a product lock table in memory. The distributed software contains a plurality of entitlement verification triggers. Each trigger is a single machine instruction in the object code, identifying a product number of the software module. When a trigger is encountered during execution, the computer checks the product lock table entry corresponding to the product number of the software. If the product is entitled to run, execution continues normally; otherwise execution is aborted. Because this verification involves only a single machine instruction, it can be done with virtually no impact to overall system performance. As a result, it is possible to place a substantial number of such entitlement verification triggers in the object code, making it virtually impossible for someone to alter the code by "patching" the triggers. The triggering instruction may alternatively perform some useful work in parallel with entitlement verification.

11/AB/78   (Item 17 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

A laser energy microinscribing system, including a semiconductor excited Q-switched solid state laser energy source; a cut gemstone mounting system, allowing optical access to a mounted workpiece; an optical system for focusing laser energy from the laser energy source onto a cut gemstone; a displaceable stage for moving said gemstone mounting system with respect to said optical system so that the focused laser energy is presented to desired positions on the gemstone, having a control input; an imaging system for viewing the gemstone from a plurality of vantage points; and a rigid frame supporting the laser, the optical system and the stage in fixed relation, to resist differential movements of the laser, the optical system and the stage and increase immunity to vibrational misalignments. The laser energy source is preferably a semiconductor diode excited Q-switched Nd:YLF

laser with a harmonic converter having an output of about 530 nm. The system may further include an input for receiving marking instructions; a processor for controlling the displaceable stage based on the marking instructions and the imaging system, to selectively generate a marking based on the instructions and a predetermined program; and a storage system for electronically storing information relating to images of a plurality of workpieces. A secure certificate of authenticity of a marked workpiece is also provided.

11/AB/79   (Item 18 from file: 654)

ABSTRACT

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

11/AB/80   (Item 19 from file: 654)

ABSTRACT

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

11/AB/81   (Item 20 from file: 654)

ABSTRACT

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain

the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

11/AB/82   (Item 21 from file: 654)

ABSTRACT

The present invention provides systems and methods for electronic commerce including secure transaction management and electronic rights protection. Electronic appliances such as computers employed in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Secure subsystems used with such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Secure distributed and other operating system environments and architectures, employing, for example, secure semiconductor processing arrangements that may establish secure, protected environments at each node. These techniques may be used to support an end-to-end electronic information distribution capability that may be used, for example, utilizing the "electronic highway."

11/AB/83   (Item 22 from file: 654)

ABSTRACT

An automated system checks networked computers, such as computers on the internet, for watermarked audio, video, or image data. A report listing the location of such audio, video or image data is generated, and provided to the proprietor(s) thereof identified by the watermark information.

11/AB/84   (Item 23 from file: 654)

ABSTRACT

An identification code signal is impressed on a carrier to be identified (such as an **electronic** data signal or a physical medium) in a manner that permits the identification signal later to be discerned and the carrier thereby identified. The method and apparatus are characterized by robustness despite degradation of the encoded carrier, and by permeation of the identification signal throughout the carrier.

11/AB/85   (Item 24 from file: 654)

ABSTRACT

A given data object can effectively contain both a graphical representation
to a network user and embedded information, such as the URL address of
another network node, thereby to permit the object itself to serve as an
automated hot link. The underlying development tools and web site browsers
create and identify such an object for use in a manner similar to a hot
link, as provided on the World Wide Web.

11/AB/86   (Item 25 from file: 654)

ABSTRACT

An embedded multi-bit signal is steganographically detected from empirical
data, such as image or audio data, and some aspect of a related system's
operation is controlled in accordance therewith. One application of the
invention is a video playback or recording device that is controlled in
accordance with the embedded multi-bit signal to limit playback or
recording operations. Another is a photo-duplication kiosk that recognizes
certain steganographic markings in an image being copied and interrupts the
copying operation.

11/AB/87   (Item 26 from file: 654)

ABSTRACT

Technology is now available permitting consumers to make amateur-or even
professional-grade copies of photographs. For wedding and portrait
photographers, in particular, the business of making duplications is
fundamental to their livelihoods. The threat of such copying is felt
strongly. To redress these concerns, a machine-readable marking is provided
on emulsion films, photographic papers, and the like. The marking encodes
digital information, yet is essentially imperceptible to the human eye. A
photographic duplication kiosk can be constructed to read this embedded
information and, if warranted by the embedded information, to disable the
kiosk's copying function. An exemplary embodiment pre-exposes the
photographic product with a spatial domain representation of the embedded
data, and may include rotationally symmetric one-or two-dimensional
patterns. Numerous other implementations are similarly practical.

11/AB/88   (Item 27 from file: 654)

ABSTRACT

An identification code signal is impressed on a carrier to be identified
(such as an **electronic** data signal or a physical medium) in a manner that
permits the identification signal later to be discerned and the carrier
thereby identified. The method and apparatus are characterized by
robustness despite degradation of the encoded carrier, and by holographic
permeation of the identification signal throughout the carrier. An
exemplary embodiment is a processor that embeds the identification signal
onto a carrier signal in real time.

11/AB/89   (Item 28 from file: 654)

ABSTRACT

A method and apparatus is provided in a data processing system for securing

access to particular files which are stored in a computer-accessible memory media. A file management program is provided as an operating system component of the data processing system. A plurality of files are stored in a computer-accessible memory media, including at least one encrypted file and at least one unencrypted file. For each encrypted file, a preselected portion of the file is recorded in memory, a decryption block is generated which includes information which can be utilized to **decrypt** the file, and the decryption block is incorporated in the file in lieu of the preselected portion which has been recorded in memory. Then, a file management program is utilized to monitor data processing system calls for files stored in the computer-accessible memory media. The file management program determines whether the called file has an associated decryption block. The called file is processed in a particular manner dependent upon whether or not the called file has an associated decryption block.

11/AB/90   (Item 29 from file: 654)

ABSTRACT

A method and apparatus is provided for distributing a software object from a source to a user. A software object is encrypted with an encryption operation utilizing a long-lived encryption key. It is directed from the source to the user. It is loaded onto a user-controlled data processing system having a particular configuration. A numerical machine identification is derived based at least in part upon the particular data processing system configuration of the user-controlled data processing system. A temporary key is derived which is based at least in part upon the numerical machine identification and the long-lived encryption key. The long-lived key generator is provided for receiving the temporary key and producing the long-lived encryption key. The user is allowed to utilize the temporary key for a prescribed interval to generate the long-lived encryption key to access the software object.

11/AB/91   (Item 30 from file: 654)

ABSTRACT

A **digital** signal is imperceptibly embedded into an input source signal, such as an image or video signal, to produce an encoded (sometimes termed "watermarked") signal. The principle of quasi-rotational symmetry is employed to facilitate detection of the embedded signal notwithstanding rotation of the encoded signal. Single or multiple degrees of symmetry can be employed. In another aspect, the **digital** signal is transformed to a frequency domain and phase-only filtered prior to its combination with the input source signal. In an illustrative embodiment, this filtering operation helps hide the **digital** signal within the source signal, and facilitates detection of the embedded **digital** signal even after the encoded signal has undergone various forms of corruption.

11/AB/92   (Item 31 from file: 654)

ABSTRACT

An identification code signal is hidden in a carrier signal (such as an **electronic** data signal or a physical medium) in a manner that permits the identification signal later to be discerned. The carrier signal can thereby be identified, or some machine responsive action can thereby be taken. In one image steganography embodiment, the relative strength of the identification code signal is both perceptually adapted in accordance with psychovisual characteristics of the image, and globally scaled in accordance with a user-set visibility control. The technique can be applied

in video imagery embodiments to control associated video equipment, e.g. to serve as a copy control signal.

11/AB/93   (Item 32 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

A method and apparatus is provided in a data processing system for securing access to particular files which are stored in a computer-accessible memory media. A file management program is provided as an operating system component of the data processing system. At least one encrypted file and at least one unencrypted file are stored in the computer-accessible memory media. An unencrypted security stub is associated with each of the encrypted files. The security stub is at least partially composed of executable code. The file management program is utilized to monitor data processing calls for a called file stored in the computer-accessible memory media. The file management program determines what the called file has an associated unencrypted security stub. The called file is processed in a particular manner dependent upon whether or not the called file has an associated unencrypted security stub.

11/AB/94   (Item 33 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

An identification code signal is impressed on a carrier to be identified (such as an **electronic** data signal or a physical medium) in a manner that permits the identification signal later to be discerned and the carrier thereby identified. The method and apparatus are characterized by robustness despite degradation of the encoded carrier, and by permeation of the identification signal throughout the carrier.

11/AB/95   (Item 34 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

A method and apparatus is provided for distributing software objects from a producer to a potential user. The software object is reversibly functionally limited, preferably through encryption, and loaded onto a computer-accessible memory media along with the file management program. The computer-accessible memory media is shipped from the producer to the potential user. The file management program is loaded into a user-controlled data processing system, and associated with the operating system for the user-controlled data processing system. The computer-accessible memory media is read with the user-controlled data processing system. The file management program is utilized to restrict access to the software object.

11/AB/96   (Item 35 from file: 654)
DIALOG(R)File 654:(c) format only 2001 The Dialog Corp. All rts. reserv.

ABSTRACT

An identification code signal is impressed on a carrier to be identified (such as an **electronic** data signal or a physical medium) in a manner that permits the identification signal later to be discerned and the carrier thereby identified. The method and apparatus are characterized by robustness despite degradation of the encoded carrier, and by permeation of the identification signal throughout the carrier.

ABSTRACT

A method and apparatus is provided in a data processing system for securing
access to particular files which are stored in a computer-accessible memory
media. A file management program is provided as an operating system
component of the data processing system. A plurality of files are stored in
a computer-accessible memory media, including at least one encrypted file
and at least one unencrypted file. For each encrypted file, a preselected
portion of the file is recorded in memory, a decryption block is generated
which includes information which can be utilized to **decrypt** the file, and
the decryption block is incorporated in the file in lieu of the preselected
portion which has been recorded in memory. Then, a file management program
is utilized to monitor data processing system calls for files stored in the
computer-accessible memory media. The file management program determines
whether the called file has an associated decryption block. The called file
is processed in a particular manner dependent upon whether or not the
called file has an associated decryption block.

ABSTRACT

An exceptionally dense information encoding system, with 4-10 times the
density of CD ROM diskettes, employs colored areas in the form of bars or
checkerboard matrices of colored dot regions to **encode** information
including alphanumerics, with each colored region being variable as to both
color and intensity. In one embodiment, so-called super pixel dots have
differently colored sub-regions within them, arranged with side-by-side
colors or with colored regions stacked one on top of the other, such that
information from one dot has as many color variables as there are stacked
layers or mixed colors. In one embodiment the super pixel dot is 5 microns
in diameter with 2 micron spacing between adjacent dots. For each color in
one embodiment there are as many as 64 intensities yielding a coding system
of high information density. The various colors are read out at one super
pixel dot position by dividing out reflected or transmitted energy from a
dot by color filtering such that a color and intensity can be detected for
each color intensity within the super pixel dot. The code provided by the
subject system is substantially invisible to the naked eye, with machine
vision and computer analysis of the information being required to
effectively **decode** differences of intensity. Additionally, encrypting can
be performed on the digitally encoded information to further hide the
information carried by the colored dot matrix. Moreover, standardized
intensities are established by one or more of the coded regions to assist
in machine decoding, and correction techniques are applied for variations
in detected color and intensity.

ABSTRACT

A method and apparatus is provided for transferring encrypted files from a
source computer to one or more target computers. An export program is
provided in the source computer and an import program is provided in the
target computer. The export program decrypts the encrypted file and tags
the export operation with an export counter value. The clear text file is
then encrypted with an encryption operation utilizing a key which is unique
to a transfer memory media, such as diskette serial number. The memory
media is carried to a target computer which utilizes the import file to
decrypt the encrypted file.

11/AB/100   (Item 39 from file: 654)

ABSTRACT

Encrypted data objects are distributed via a broadcast communication channel or media. Relatively large access indicia may also be pre-distributed to any potential data object users and/or purchasers via an access communication channel or media. Subsequently, when a particular potential user or purchaser wishes to **decrypt** a given data object, he or she communicates to a data distribution point the identity of the desired data object and the identity of a valid access incidium. A relatively short decryption key is then furnished via a key distribution communication channel or media to permit decryption while at the same time permitting appropriate accounting operations to take place. The system is resistant to abuse in several ways but in part because such abuse would be approximately as difficult as would be re-distribution of the entire decrypted data object itself.

11/AB/101   (Item 40 from file: 654)

ABSTRACT

An exceptionally dense information encoding system, with 4-10 times the density of CD ROM diskettes, employs colored areas in the form of bars or checkerboard matrices of colored dot regions to **encode** information including alphanumerics, with each colored region being variable as to both color and intensity. In one embodiment, so-called super pixel dots have differently colored sub-regions within them, arranged with side-by-side colors or with colored regions stacked one on top of the other, such that information from one dot has as many color variables as there are stacked layers or mixed colors. In one embodiment the super pixel dot is 5 microns in diameter with 2 micron spacing between adjacent dots. For each color in one embodiment there are as many as 64 intensities yielding a coding system of high information density. The various colors are read out at one super pixel dot position by dividing out reflected or transmitted energy from a dot by color filtering such that a color and intensity can be detected for each color intensity within the super pixel dot. The code provided by the subject system is substantially invisible to the naked eye, with machine vision and computer analysis of the information being required to effectively **decode** differences of intensity. Additionally, encrypting can be performed on the digitally encoded information to further hide the information carried by the colored dot matrix. Moreover, standardized intensities are established by one or more of the coded regions to assist in machine decoding, and correction techniques are applied for variations in detected color and intensity.

11/AB/102   (Item 41 from file: 654)

ABSTRACT

An integrated software **piracy** prevention system incorporates several characteristic identification codes identifying installation and software components. A separate security device is attached to and in communication with the protected computer system. It is interactively queried regarding proper authorization of the current user. This approach is unusually flexible and provides economical tracking of licensees and their use of sophisticated programs.

11/AB/103   (Item 42 from file: 654)

ABSTRACT

Method and apparatus which restricts software, distributed on **magnetic media**, to use on a single computing machine. The original medium is functionally uncopyable, until it is modified by the execution of a program stored in a tamper proof co-processor which forms a part of the computing machine. The modified software on the original medium may then be copied, but the copy is operable only on the computing machine containing the co-processor that performed the modification.

?